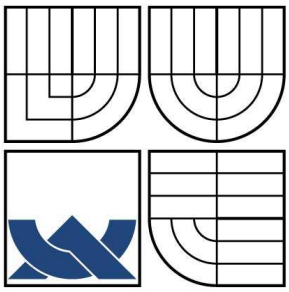
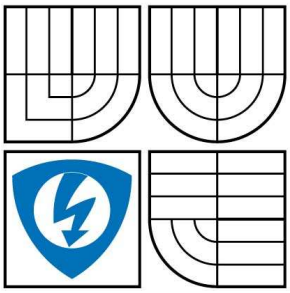


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

NÁVRH VIRTUÁLNÍ LOKÁLNÍ POČÍTAČOVÉ SÍTĚ PRO EDUKATIVNÍ ÚČELY

DESIGN OF A VIRTUAL LOCAL COMPUTER NETWORK FOR EDUCATIONAL PURPOSES

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE BC. MARTIN JANOŠÍK
AUTHOR

VEDOUCÍ PRÁCE DOC. ING. VLADISLAV ŠKORPIL, CSC.
SUPERVISOR

BRNO 2008

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Bc. Martin Janošík

Bytem: Střední Novosadská 183/39A,
Olomouc - Nové Sady, 779 00

Narozen/a (datum a místo): 11.4.1984, Olomouc

(dále jen „autor“)

a

2. Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií

se sídlem Údolní 244/53, 602 00, Brno

jejímž jménem jedná na základě písemného pověření děkanem fakulty:

prof. Ing. Kamil Vrba, CSc.

(dále jen „nabyvatel“)

Čl. 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   - ☐ disertační práce
   - ☑ diplomová práce
   - ☐ bakalářská práce
   - ☐ jiná práce, jejíž druh je specifikován jako.....

(dále jen VŠKP nebo dílo)

Název VŠKP: Návrh virtuální lokální počítačové sítě pro edukativní účely

Vedoucí/ školitel VŠKP: doc. Ing. Vladislav Škorpil, CSc.

Ústav: Ústav telekomunikací

Datum obhajoby VŠKP: ……..

VŠKP odevzdal autor nabyvateli v:

- ☑ tištěné formě – počet exemplářů 2
- ☑ elektronické formě – počet exemplářů 1

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.

3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - ☑ ihned po uzavření této smlouvy
   - ☐ 1 rok po uzavření této smlouvy
   - ☐ 3 roky po uzavření této smlouvy
   - ☐ 5 let po uzavření této smlouvy
   - ☐ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: ……..

…….. ……

Nabyvatel Autor

ANOTACE

Práce se zabývá návrhem virtuální lokální počítačové sítě pro laboratorní využití. Cílem je navrhnout a zrealizovat vhodné zapojení sítě pro monitorování uvažovaných datových toků. Pomocí síťových analyzátorů (softwarový ClearSight a hardwarový NetTool Serie II) detailně sledovat využívané přenosové protokoly vrstev TCP/IP. Rozhodující je především správná volba odpovídajících síťových prvků a jejich přesná konfigurace. Následně je vypracován návrh laboratorní úlohy pro potřebu výuky studentů bezprostředně související s danou problematikou. Její zadání poslouží vyučujícímu jako předloha pro měření. Výsledky zpracované ve formě vzorového protokolu umožní pozdější porovnání naměřených dat. Dalším úkolem je vypracování přehledných manuálů k používaným síťovým analyzátorům.

Klíčová slova: virtuální počítačové sítě (VLAN), IP telefonie (VoIP), architektura TCP/IP, protokoly SIP, RTP, RTCP, monitorování a analýza datových přenosů

ABSTRACT

The master's thesis focuses on the virtual local computer network for laboratory usage. It aims to propose and realize proper network connection in order to monitor expected data flow. Thanks to the network analysers (software ClearSight and hardware NetTool Series II) it plans to pursue in detail the used transmission protocols of TCP/IP layers. The most decisive feature happens to be the right choice of appropriate network components and their precise configuration. Consequently, the thesis formulates a proposal of a laboratory task for the needs of students, which is also closely related to the actual problems. The assignment of the task will serve the teachers as a test pattern for measurement. The results elaborated in the form of the model protocol should enable later comparison of the recorded data. Another part of the diploma thesis is the working-out of well arranged manuals for the network analysers involved.

Keywords: Virtual Local Area Network (VLAN), Voice over Internet Protocol (VoIP), TCP/IP architecture, Session Initiation Protocol (SIP), Real-time Transport Protocol (RTP), Real-time Transport Control Protocol (RTCP), monitoring and analyses data transmission

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Návrh virtuální lokální počítačové sítě pro edukativní účely“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.“

V Brně dne ....

podpis autora

PODĚKOVÁNÍ

Děkuji vedoucímu diplomové práce doc. Ing. Vladislavu Škorpilovi CSc. a odbornému konzultantovi Ing. Michalu Polívkovi za velmi užitečnou metodickou pomoc a cenné rady při zpracování této diplomové práce.

V Brně dne ....

podpis autora

Obsah

ÚVOD

Úkolem této diplomové práce je vytvořit vhodnou počítačovou síť pro edukativní účely, která bude zahrnovat problematiku virtuálních sítí (VLAN) a provést následnou analýzu datového provozu v této síti. Analýze budou podrobeny zejména hovory uskutečněné pomocí IP telefonů, zaměření na protokoly SIP a RTP, a také data běžného síťového provozu využívající protokoly jako jsou: HTTP, POP, SMTP, FTP atd.

Zachytávání paketů bude uskutečněno pomocí nového ClearSight softwarového analyzátoru, který umožňuje podrobný rozbor rámců rozdělených do příslušných síťových vrstev, a také hardwarovým příručním FLUKE NetTool Serie II analyzátorem připojeným přímo mezi příslušná zařízení.

Na přepínači (switch) jsou vytvořeny dvě virtuální počítačové sítě. Jedna slouží pro datový provoz počítačů v laboratoři, druhá je určena pro přenos hlasu připojených IP telefonů. Součástí počítačové sítě je server s VoIP softwarovou ústřednou, která obsluhuje připojené IP telefony. Zbývající komunikace web, e-mail a FTP serverů je uskutečněna přes školní LAN do sítě internet.

Výstupem této práce je stručné a výstižné zadání úlohy, které poslouží studentům jako předloha pro měření v laboratoři. K porovnání výsledků zaznamenaných studenty pomůže vyučujícímu vypracovaný vzorový protokol, doplněný o řadu reportů exportovaných z analyzátorů.

1. TEORETICKÝ PŘEHLED

1.1 VLAN

Termín virtuální síť se používá pro skupinu síťových zařízení, která jsou libovolně propojena počítačovou sítí a chovají se stejně jako by byly na společném fyzickém médiu odděleném od zbývající části sítě. Virtuální sítě tak umožňují propojit vzdálená zařízení a zároveň je oddělit od jiných virtuálních sítí. Segmenty lokální sítě, ve kterých se šíří všesměrové vysílání, tak nejsou omezeny fyzickými spoji, ale mohou být definovány libovolně dle potřeby. Virtuální sítě segmentují velké sítě do logických celků, které vystupují jako nezávislé lokální sítě. Rozdělení sítě lze použít pro omezení šíření všesměrového vysílání a také je často nutné z bezpečnostních a administrativních důvodů. Vhodným dělením sítě na menší celky lze snadněji zvládnout celkový provoz a zátěž sítě.

Virtuální sítě samozřejmě nelze vytvářet bez odpovídajících aktivních prvků, přepínačů a směrovačů. Ty je možné propojit jediným spojem a jejich software zajistí komunikaci samostatných sítí se stejnými čísly (tagy). V principu se jedná o nadstavbu nad běžným ethernetovým protokolem. K běžným paketům je připojena informace o čísle virtuální sítě (tag), kterou protější zařízení využije k rozpoznání příslušnosti k síti. Nejrozšířenější normou VLAN je tagovací protokol IEEE 802.1Q [1].

1.1.1 Standard IEEE 802.1Q

Definuje formát přenosu informací o členství ve virtuální sítí a protokol pro přenos informací o definovaných virtuálních sítích mezi přepínači. Pokud podporují přepínače tento standard, pak stačí pro propojení virtuálních sítí vytvořených v těchto přepínačích pouze jeden spoj [2], [3].

Struktura rámce 802.1Q

7	*1*	*6*	*6*	*2*	*2*	*2*	*42-1496*	*4*
PRE	SFD	DA	SA	TPID	TCI	L/T	Data	CRC

Obr. 1.1: Rámec 802.1Q

- **PRE** – 7 bytů. Úvodní sekvence sestává ze střídajících se 1 a 0, které indikují přijímacím stanicím příchozí rámec a slouží k synchronizaci obvodů fyzické vrstvy s proudem bitů.
- **SFD (Start of Frame Delimiter)** – začátek oddělovače informací – 1 byte. Jedná se o střídající se sekvence 1 a 0. Dvě po sobě jdoucí 1 indikují, že další bit je nejvyšší bit nejvyššího bytu cílové adresy
- **DA (Destination address)** – cílová adresa – 6 bytů. Políčko DA identifikuje, která stanice (případně které stanice) má rámec přijmout
- **SA (Source address)** – adresa odesílatele – 6 bytů
- **TPID** – Nabývá hodnoty 8100h pro rámce přenášející značku IEEE 802.1Q/802.1P
- **TCI** – Tag Control Informatik

3b	*1b*	*12b*
User Priority	CFI	VLAN ID (VID)

Obr. 1.2: Rozdělení TCI

  - **User Priority** – Určena priorita pro L2 QoS/CoS

- **CFI** – Canonical Format Indicator – definuje pořadí, v jakém jsou přenášeny bity ve vnitřní části rámce. Pro hodnotu 0 se jedná o little endian (použití v ethernetu), pro hodnotu 1 o big endian (použití v FDDI a Token Ringu).
- **VID –** VLAN ID identifikace VLAN, která je užita standardem 802.1Q a sestává z 12 bitů. Umožňuje identifikaci až 4094 VLAN, přičemž VID 0 slouží k identifikaci přednostních rámců a VID 4095 je rezerva.

- **Length/Type** – 2 byty. Určuje buď délku dat v rámci, nebo rámcový typ, používá-li rámec volitelný formát.
- **Data** – Posloupnost 42 až 1496 bytů. Minimum celkového rámce je 64 bytů.
- **CRC** – 4 byty – kontrolní součet.

1.2 Architektura TCP/IP

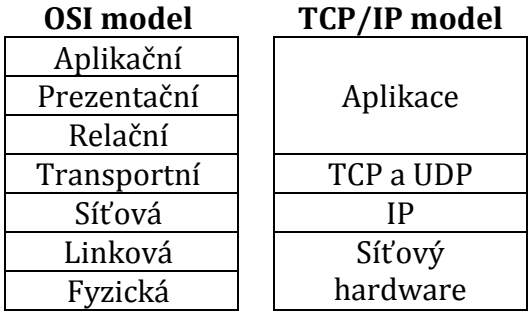
TCP/IP je označení dvou přenosových protokolů, používaných v počítačových sítích TCP (primární transportní protokol) a IP (protokol síťové vrstvy). Ve skutečnosti TCP/IP značí nejznámější protokoly z celé sady protokolů. Přenosový protokol je soubor pravidel, kterými se řídí počítače, aby se mohly přes síť dorozumět. Počítač musí vyslat data do sítě určitým způsobem a v daném tvaru, aby ostatní počítače byly schopny data přijmout, přečíst a zpracovat.

Vzhledem ke složitosti problémů je síťová komunikace rozdělena do tzv. vrstev, které znázorňují hierarchii činností. Výměna informací mezi vrstvami je přesně definována. Každá vrstva využívá služeb vrstvy nižší a poskytuje své služby vrstvě vyšší.

Komunikace mezi stejnými vrstvami dvou různých systémů je řízena komunikačním protokolem za použití spojení vytvořeného sousední nižší vrstvou. Architektura umožňuje výměnu protokolů jedné vrstvy bez dopadu na ostatní. Příkladem může být možnost komunikace po různých fyzických médiích – ethernet, token ring, sériová linka [4], [5].

Architektura TCP/IP je členěna do čtyř vrstev na rozdíl od referenčního modelu OSI se sedmi vrstvami (orb. 1.3):

- aplikační vrstva (application layer)
- transportní vrstva (transport layer)
- síťová vrstva (network layer)
- vrstva síťového rozhraní (network interface layer)



Obr. 1.3: Srovnání modelů OSI a TCP/IP

1.2.1 Praktický pohled na vrstvový model

Budeme-li přenášet pomocí protokolu FTP čistý textový soubor „pozdrav.txt“ od klienta na server obsahující text: „dobrý den“ bude komunikace mezi FTP serverem a klientem zahrnovat několik rámců pro sestavení spojení, výpis adresářové struktury apod. Vzhledem k délce přenášených dat bude možné přenést celý soubor jedním rámcem. Ten bude po zobrazení v šestnáctkové soustavě vypadat jako na obr. 1.4. Samotnému přenosu souboru bude předcházet výměna informací jednotlivých vrstev [6].

```
00 13 d4 b0 e7 b1 00 e0 98 3c 25 0e 08 00 45 00 00 3d 16
b5 40 00 80 06 60 b1 c0 a8 01 03 c0 a8 01 01 0a 96 0a 61
4b ae 5d 04 51 eb 42 e2 80 18 44 70 f1 88 00 00 01 01 08
0a 00 03 ec 49 00 18 e8 19 64 6f 62 72 fd 20 64 65 6e
```

Obr. 1.4: Kompletní rámec. Data jsou přenášena za sebou po řádcích

Jak je možné vidět na obr. 1.5, každý protokol vyšší vrstvy je zapouzdřen v protokolu vrstvy předchozí – nižší [6].

```
00 13 d4 b0 e7 b1 00 e0 98 3c 25 0e 08 00 45 00 00 3d 16 b5 40 00 80 06 60 b1 c0 a8 01 03 c0 a8 01 01 0a
96 0a 61 4b ae 5d 04 51 eb 42 e2 80 18 44 70 f1 88 00 00 01 01 08 0a 00 03 ec 49 00 18 e8 19 64 6f 62 72
fd 20 64 65 6e
```

Ethernetový rámec

00 13 d4 b0 e7 b1 – MAC (hardwarová) adresa síťové karty cílového uzlu
00 e0 98 3c 25 0e – MAC (hardwarová) adresa síťové karty zdrojového uzlu
08 00 – identifikace protokolu vyšší vrstvy, v tomto případě protokolu IP

IP protokol

45 – verze IP protokolu, v tomto případě IP verze 4
00 – oddělovací pole
00 3d – celková délka IP paketu, v tomto případě 61
16 b5 – identifikace svazuje fragmenty IP paketů
40 – příznaky
00 – odstup fragmentu (fragment offset)
80 – doba platnosti (TTL – time to live)
06 – identifikace protokolu vyšší vrstvy, v tomto případě TCP protokolu
60 b1 – kontrolní součet hlavičky
c0 a8 01 03 – IP adresa zdrojového uzlu, v tomto případě 192.168.1.3
c0 a8 01 01 – IP adresa cílového uzlu, v tomto případě 192.168.1.1

TCP protokol

0a 96 – zdrojový TCP port, v tomto případě 2710
0a 61 – cílový TCP port, v tomto případě 2657
4b ae 5d 04 – sekvenční číslo
51 eb 42 e2 – potvrzovací číslo
80 – délka TCP hlavičky, v tomto případě (80h = 128d ⇒ 128/4 = 32bajtů)
18 – příznaky TCP paketu
44 70 – velikost okna
f1 88 – kontrolní součet pseudohlavičky
00 00 – oddělení
01 01 08 0a 00 03 ec 49 00 18 e8 19 – volby, kde 08 0a 00 03 ec 49 00 18 e8 19 je časovým otiskem

Data

64 6f 62 72 fd 20 64 65 6e – data, v tomto případě, „dobrý den“

Obr. 1.5: Popis reálného provozu na síťovém rozhraní TCP/IP, Ethernet

1.3 Vrstvy TCP/IP

1.3.1 Aplikační vrstva

Tato vrstva je čtvrtou a nejvyšší vrstvou TCP/IP. Jejími částmi jsou jednotlivé aplikační programy, které na rozdíl od referenčního modelu ISO/OSI přímo komunikují s transportní vrstvou. Prezenční a relační služby, které zajišťují samostatné vrstvy obsažené v modelu ISO/OSI, si musí jednotlivé aplikace realizovat sami.

Aplikační vrstva je nejbohatší na počet obsažených protokolů v jednotlivých vrstvách TCP/IP modelu např. RSVP, RTP, RTSP, SIP [7].

RSVP – signalizační protokol umožňující přijímací stanici reservovat dostatečnou šíři pásma pro přenos dat citlivých na zpoždění (hlas, video)

RTP – podporuje přenos interaktivního videa či hlasu a je založen na synchronizaci časového posunu a zjištění ztráty nebo nesprávného pořadí dat.

RTSP – poskytuje rozhraní vysílaného videa mezi aplikací a serverem.

SIP – protokol zajišťující vstup individuálního uživatele do spojení bod – bod.

1.3.2 Transportní vrstva

Jde o třetí ze čtyř vrstev TCP/IP, která je nejčastěji realizována právě protokolem TCP a bývá také označována jako Transport Laser. Hlavním úkolem této vrstvy je zajistit přenos mezi dvěma koncovými účastníky. Podle nároků a požadavků koncových zařízení může transportní vrstva regulovat tok dat oběma směry, zajišťovat spolehlivost přenosu a také měnit nespojovaný charakter přenosu (v síťové vrstvě) na spojovaný. Dalším používaným protokolem na úrovni transportní vrstvy je protokol UDP, který na rozdíl od TCP nezajišťuje na úrovni transportní vrstvy spolehlivost přenosu. Jeho bezstavovost je užitečná pro servery, které obsluhují mnoho klientů nebo pro nasazení, kde se počítá se ztrátami datagramů a není vhodné, aby se ztrácel čas novým opětovným odesíláním starých (nedoručených) zpráv (např. VoIP, online hry).

Rozdíl mezi TCP a UDP

TCP je spojově orientovaný protokol. Spojení může otevřít klient nebo server a pak mohou už být posílána jakákoliv data oběma směry. Charakteristické vlastnosti TCP protokolu jsou [4], [8]:

- spolehlivost – TCP používá potvrzování o přijetí (acknowledgment), opětovné posílání (retransmission) a překročení časového limitu (timeout). TCP nepřipustí žádná ztracená data. Jestliže se některá data ztratí po cestě, server si je opětovně vyžádá. Pouze pokud několikrát po sobě vyprší časový limit, je celé spojení ukončeno.
- zachování pořadí – jestliže se odešlou dvě zprávy, první dojde vždy k serveru dříve než druhá. Pokud jsou data doručena ve špatném pořadí, TCP vrstva se postará o to, aby některá pozdržela a finálně je předala správně seřazená.
- vyšší režie – TCP protokol potřebuje tři pakety jen pro otevření spojení, což však umožňuje zaručit spolehlivost celého spojení.

UDP je jednodušší protokol založený na odesílání nezávislých zpráv. Charakteristika protokolu [8], [9]:

- bez záruky – protokol nemůže ověřit, zda data došla danému příjemci. Datagram se může po cestě ztratit. UDP neumožňuje žádné potvrzování, přeposílání ani časové limity.
- nezachovává pořadí – jestliže odešleme dvě zprávy jednomu příjemci, nemůžeme předvídat, v jakém pořadí budou doručeny.
- jednoduchost – nižší režie než u TCP (není zde řazení, žádné sledování spojení atd.).

1.3.3 Síťová vrstva

Tato vrstva již není závislá na konkrétní přenosové technologii a v terminologii TCP/IP je označována také jako Internet Layer (vrstva vzájemného propojení sítí). Je realizována pomocí protokolu IP. Úkol této vrstvy je v prvním přiblížení stejný jako úkol síťové vrstvy v referenčním modelu ISO/OSI. Stará se o to, aby se jednotlivé pakety dostaly od odesilatele až ke svému skutečnému příjemci, přes případné směrovače resp. brány. Vzhledem k nespojovanému charakteru přenosů v TCP/IP je na úrovni této vrstvy zajišťována jednoduchá (tj. nespolehlivá) datagramová služba [7].

1.3.4 Vrstva síťového rozhraní

Vrstva síťového rozhranní je nejnižší vrstvou TCP/IP a má na starosti vše, co je spojeno s ovládáním konkrétní přenosové cesty resp. sítě s přímým vysíláním a příjmem paketů. Provádí zapouzdření IP datagramu do rámců, přidělení IP adresy adresám fyzickým tzv. MAC adresám, které jsou dále poslány po síti. V rámci soustavy TCP/IP není tato vrstva blíže specifikována, neboť závisí na použité přenosové technologii [10].

1.4 VoIP

Voice over Internet Protocol je technologie umožňující přenos digitalizovaného hlasu v těle paketů rodiny protokolů UDP/TCP/IP prostřednictvím počítačové sítě nebo jiného média, prostupného pro protokol IP. Využívá se pro telefonování prostřednictvím internetu, intranetu nebo jakéhokoliv jiného datového spojení. Nutnou podmínkou pro srozumitelné a spolehlivé VoIP telefonní spojení je zajištění tzv. kvality služby, zkráceně označované QoS (Quality of Service) .

1.4.1 Protokoly VoIP

Pro přenos hlasu se používá na třetí vrstvě OSI modelu protokol IP, na čtvrté vrstvě protokol UDP. V těle jednotlivých UDP datagramů se kromě dalších údajů přenáší malý úsek telefonního hovoru. Je zakódovaný podle určitého pravidla (algoritmu), aby se dosáhlo úspory objemu přenášených dat. Kódovací a dekódovací algoritmy, zkráceně kodeky, mají různá označení (G.711, G.723, G.729, atd.) jsou standardizovány a ze značné části i patentovány. Kromě UDP datagramů, nesoucích o vrstvu výš v RTP zapouzdřené úseky vlastního hovoru, zahrnuje VoIP přenos ještě další pakety. Jsou to

např. ICMP pakety a také datagramy TCP a UDP. Ty řídí přenos, nesou telefonní signalizaci, ověřují dostupnost komunikujících zařízení.

Celá rodina VoIP protokolu není jediná, ale má řadu variant, lišících se podle standardu, použitého pro VoIP spojení. V současnosti jsou nejběžnější H.323 a SIP. Používají se i speciální firemní protokoly, jako např. Skinny (firmy Cisco) nebo HFA (firmy Siemens). Obecně lze říct, že všechny protokoly mají podobný přenos hovoru pomocí proudu krátkých úseků nesených v RTP, ale liší se ve službách a signalizaci.

Hovor je přenášen v paketech, které používají standard Real Time Protocol. Každý RTP paket obsahuje kousek digitalizovaného hovoru. Když se v přijímacím IP telefonu spojí několik RTP paketů, vytvoří slovo. Linky pro přenos hlasu se připojí přímo mezi telefony a brány. Hovor neprochází přes server ani není přenášen signálovými protokoly.

Nejsložitější a nejvíce pokročilý (protože je nejstarší) je pravděpodobně protokol H.323, nejvíce perspektivní a v současné době nejvíce používaný je protokol SIP – Session Initiation Protocol (protokol pro inicializaci relací). Velkou výhodu má SIP např. v tom, že prochází bez větších potíží přes místo, kde v síti probíhá překlad adres NAT. Existuje několik způsobů, jak dosáhnout průchodu komunikace typu SIP přes problémová místa v síti [11].

1.4.2 Protokol SIP

Je signalizační protokol řízený aplikační vrstvou a je jednou z alternativ pro realizaci hlasového přenosu a pro internetové konference s jedním nebo více účastníky spojených v rámci IP sítě. SIP je navržen jako protokol nezávislý na protokolech nižší transportní vrstvy (TCP, UDP, ATM, X.25). Má svůj systém k zabezpečení bezchybného přenosu. SIP není svázán s žádnými konkrétními protokoly pro vlastní přenos multimediálních dat. Uvnitř zprávy protokolu SIP pro navázání spojení je proto zapouzdřena zpráva jiného protokolu, který specifikuje použitá kódování pro multimediální data, jejich parametry a čísla portů, na kterých mají být data vysílána nebo přijímána. Obvykle se pro tento účel používá protokol SDP. Protokol SIP plní také funkci registrace uživatelů, která umožňuje používat pro identifikaci uživatelů logické adresy nezávislé na fyzickém umístění uživatele. SIP transparentně podporuje mapovací a směrovací služby. Spojení může představovat obecně jakýkoliv multimediální přenos. V praxi je ale SIP nejčastěji využíván pro telefonování po IP síti [10], [12].

Tento signalizační protokol má následující vlastnosti :

- SIP adresy jsou typu URL: user@host
- User může být jméno, telefon, číslo
- Hostem může být doména nebo IP adresa
- Uživatelé nebo klienti se registrují u SIP serverů, aby jim poskytli kontaktní informace

1.4.3 Protokol RTP

Přenosový protokol v reálném čase je protokol zajišťující podporu pro koncové multimediální přenosy online. Nezaručuje doručení dat ani správné pořadí jednotlivých paketů (to záleží na momentálních možnostech sítě), ale definuje jejich pořadová čísla, podle kterých mohou multimediální aplikace rozpoznat chybějící pakety. Zakládá se na synchronizaci časového přenosu a zjištění ztráty nebo nesprávného pořadí dat. RTP nejčastěji používá protokol UDP (čísla portů 5004, 5005, 6970), ale může využít i jiné protokoly. Bezpečnou variantu RTP představuje protokol SRTP (Secure Real-time Transport Protocol).

RTP protokol byl navržen jak pro individuální, tak pro skupinové přenosy, pro jednosměrný i obousměrný přenos. Je tedy použitelný pro aplikace videokonference i pro IP telefonii, používají ho protokoly SIP i H.323.

K multimediálnímu obsahu RTP připojuje záhlaví, které obsahuje pořadové číslo paketu (sequence number) pro zjištění ztrát nebo duplicity paketů a označení typu obsahu (payload identification), tj. informaci o formátu multimediálního souboru, který tvoří obsah paketu (např. JPEG, G.722, H.261). Kódování obsahu se může změnit, pokud se má přizpůsobit rozdílům v šířce pásma. Dále RTP pakety obsahují indikaci začátku a konce rámce (frame indication), identifikaci zdroje (source identification) a synchronizaci (intramedia synchronization) pro detekci různého kolísání zpoždění v rámci daného toku a pro potřebnou kompenzaci tohoto kolísání při vlastním přehrávání obrazů a zvuků.

Formát RTP datagramů je jednoduchý a obecný, takže vyhovuje všem aplikacím v reálném čase (existuje pouze jeden typ zprávy RTP). Mezi typy dat RTP zprávy jsou G.721 audio, GSM audio, G.722 audio, MPEG audio, G.728 audio, H.261, MPEG-1 video, MPEG-2 video [13], [14].

1.4.4 Protokol RTCP

Jak bylo řečeno výše, RTP neposkytuje žádný mechanizmus jak zajistit doručení paketů, jejich včasné doručení či doručení ve správném pořadí. Doručování paketů je monitorováno pomocí podpůrného řídicího protokolu RTCP. Tyto dva protokoly jsou často brány dohromady a označovány jako RTP/RTCP.

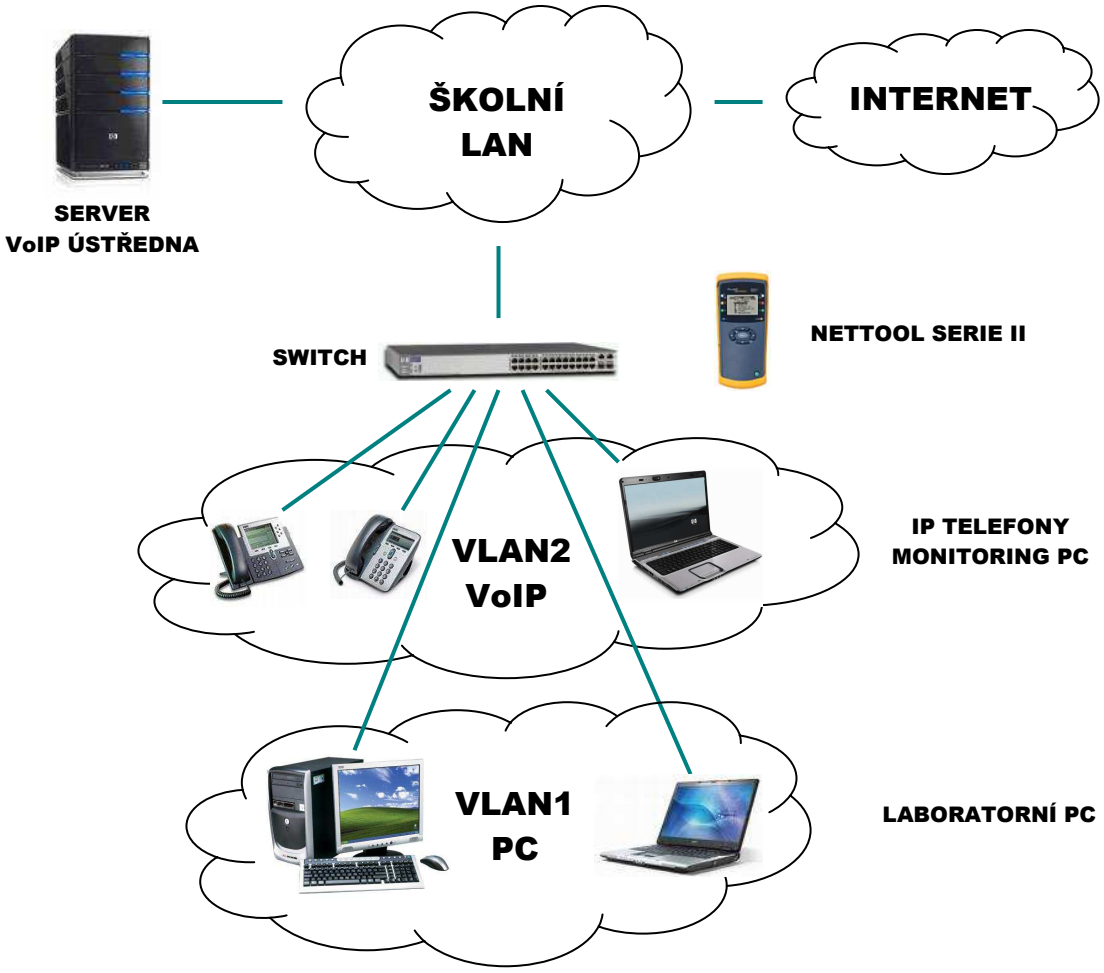
Řídicí protokol pro přenos v reálném čase (RTCP) spolupracuje s protokolem RTP. Používá periodické vysílání paketů od každého účastníka relace RTP všem ostatním účastníkům za účelem řízení výkonnosti a pro diagnostické účely. RTCP pomáhá RTP monitorovat doručení dat v rozsáhlých sítích se skupinovým vysíláním. Monitorování pomáhá příjemci detekovat ztrátu paketů a provést kompenzaci kolísání zpoždění v síti. RTCP používá UDP port o jedničku vyšší než používá RTP.

RTCP vytváří zpětnou vazbu mezi účastníky relace protokolu RTP, ve které periodicky probíhá výměna RTCP paketů. RTCP pakety obsahují informace, podle kterých může strana vysílající multimediální proud dynamicky měnit např. rychlost přenosu na základě požadavků strany přijímající. Protokol RTCP tak poskytuje služby řízení toku a kontroly zahlcení sítě [13], [15].

2. NÁVRH VIRTUÁLNÍ POČÍTAČOVÉ SÍTĚ PRO SIMULACI

Konfigurace přepínače, na kterém se vytvoří dvě virtuální počítačové sítě. Provedení celkové analýzy dat přenášených navrhnutou síti. Zaměření se na přenos hlasu pomocí IP telefonů, záznam protokolů SIP a RTP. Nastavení monitorovacího a monitorovaných portů a následný odposlech a analýza VoIP hovorů. Analýza stahovaných či nahrávaných dat některého z FTP serverů. Záznam odeslaných a přijatých e-mailů s využitím protokolů POP3 a SMTP. Surfování po internetových stránkách, analýza HTTP protokolu a puštění internetových videí využívající protokol RTSP.

2.1 Schéma zapojení:



Obr. 2.1: Schéma zapojení virtuálních LAN

2.1.1 Popis jednotlivých prvků sítě

- **Server (VoIP ústředna)** – počítač s OS Windows Server 2008, na kterém je nainstalována VoIP ústředna od společnosti 3CX, která zajišťuje správnou funkci IP telefonů v síti
- **Switch** – základní prvek celé počítačové sítě; jsou k němu připojeny všechny ostatní zařízení; realizuje spojení mezi nimi
- **VoIP telefony** – běžné IP telefony od firmy SMC podporující novější protokol SIP
- **Monitorig PC** – počítač s nainstalovaným softwarový analyzátorem ClearSight, který slouží k podrobné analýze síťového provozu
- **Laboratorní PC** - standardní stolní počítače popř. notebooky, které v laboratoři slouží k měření dalších úloh
- **NetTool Serie II** – hardwarový analyzátor, který se zapojuje přímo do sítě pomocí kabelu RJ-45 mezi jednotlivá zařízení a nebo jako koncový bod

2.2 Zadání laboratorní úlohy

1. Seznamte se s analyzátory ClearSight a NetTool; jejich manuály jsou uvedeny v kap. 5
2. Na přepínači nakonfigurujte dvě virtuální počítačové sítě – VoIP a PC (viz. kap. 3)
3. Nastavte na přepínači monitorování portů a realizujte odposlech některého z hovorů
4. Analyzujte a popište komunikaci mezi telefony a ústřednou
5. Promyslete si různé způsoby zabezpečení sítě proti neoprávněnému útoku
6. Zachyťte různé protokoly v počítačové síti a proveďte jejich podrobnou analýzu
7. Výsledky měřeni zpracujte v závěrečném protokolu s využitím reportů analyzátorů

Cílem úlohy je seznámit se s probíhající komunikací v síti během přenosu dat. Porozumět architektuře protokolů jednotlivých vrstev modelu TCP/IP. Naučit se pracovat s kvalitními síťovými analyzátory. Navrhnout zabezpečení sítě proti úniku citlivých informací.

3. POPIS A KONFIGURACE ZAŘÍZENÍ

3.1 Charakteristika přepínače HP2626

Switch (česky přepínač) je aktivní síťový prvek propojující jednotlivé segmenty sítě. Obsahuje menší či větší množství portů (až několik stovek), na něž se připojují síťová zařízení nebo části sítě. Pojem switch se používá pro různá zařízení v celé řadě síťových technologií. Obecnou vlastností switchů je, že analyzují procházející pakety a podle informací v nich obsažených (adres, identifikátorů apod.) rozhodují, kam paket předat dál.

Port-based VLAN se typicky užívají ke snížení všesměrového vysílání a k zvýšení bezpečnosti. Na switchi jsou rámce přeposílány pouze mezi porty patřícími do stejné VLAN.

U Tagged VLAN může port na switchi patřit do více VLAN zároveň, pokud připojené zařízení podporuje standard 802.1Q. Pokud tedy na takovýto port připojíme server se síťovou kartou podporující 802.1Q VLAN, může být členem více VLAN. To umožní členům různých VLAN přistupovat k tomuto serveru přes jediný kabel. Značky (tags)

slouží k rozlišení provozu rozdílných VLAN. Na obr. 1.1 je popsána struktura rámce 802.1Q.

Význam parametrů pro nastavení portů:

Untagged – Prioritně nastavený port pro danou virtuální síť

Tagged – Port může patřit do více virtuálních sítí – využívá tagy

No – Neobsažený port v dané VLAN

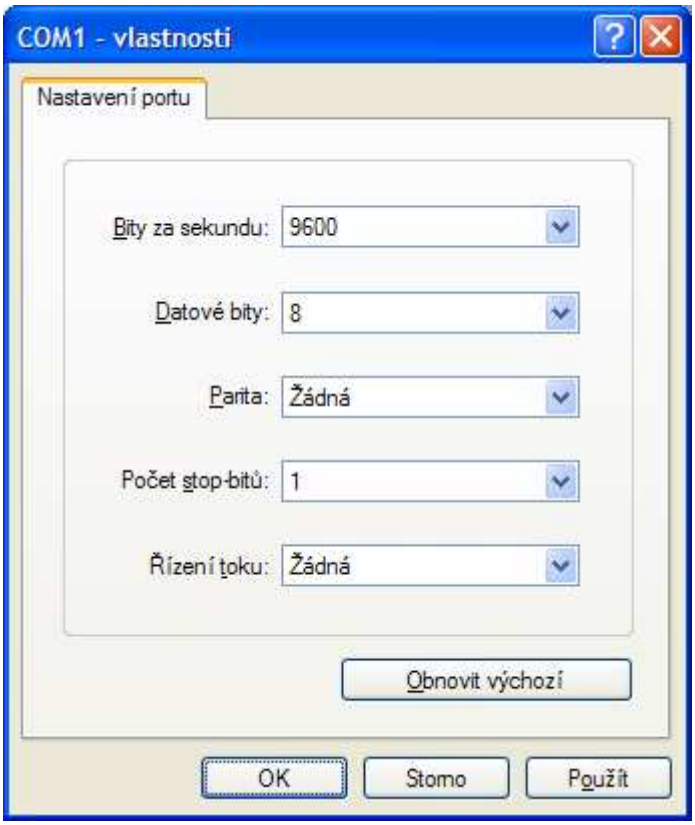
Forbit – Blokovaný port

Port monitoring (mirroring): Je funkce přepínače, která monitoruje veškerý provoz na předem definovaných portech a tyto data kopíruje na určený monitorovací port.

3.1.1 Konfigurace přepínače

Pro zapojení uvedené na obr. 2.1 je potřeba switch vhodně nakonfigurovat. Na počátku je v továrním nastavení. Přes sériové rozhraní pomocí hyperterminálu je třeba nastavit jednotlivé virtuální sítě (VLAN), také vyzkoušet konfiguraci switche přes webové rozhraní a přiřadit monitorovací stanici porty, které bude sledovat.

Pomocí hyperterminálu (Start/Všechny programy/Příslušenství/Komunikace/ Hyperterminál) se připojíme na konzoly. Vytvoříme nové připojení (název si zvolíme libovolný např. HP2626), vybereme port **COM1** a další parametry nastavíme dle obr. 3.1. Po úspěšném zadání hodnot se dostaneme do příkazové řádky terminálu. Zde příkazem **menu** se zobrazí hlavní konfigurační nabídka přepínače.



Obr. 3.1: Nastavení parametrů pro připojení k přepínači

Pod položkou **1. Status and Counters** si můžeme prohlédnout stávající nastavení a další informace o zařízení. Můžeme zde sledovat provoz na jednotlivých portech, zjistit MAC adresy zařízení připojených k těmto portům atd. Příkazem **2. Switch Configuration** se dostaneme do konfigurační nabídky přepínače obr. 3.2.

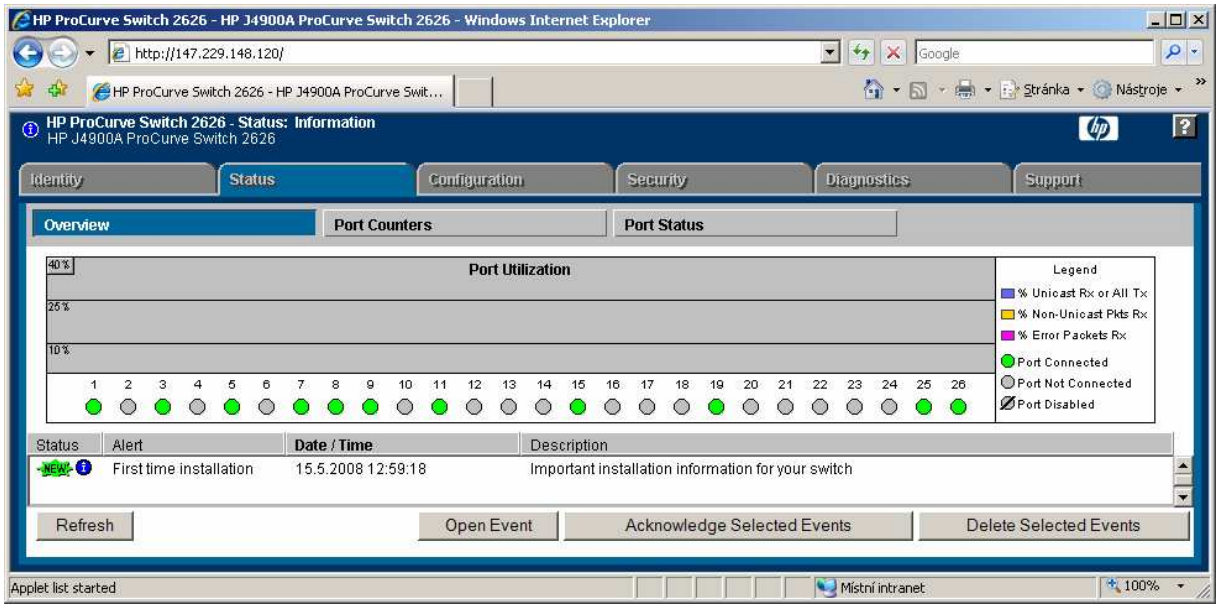
```
HP ProCurve Switch 2626                                1-Jan-1990   0:00:00
=========================- CONSOLE - MANAGER MODE -============================
                          Switch Configuration Menu

   1. System Information
   2. Port/Trunk Settings
   3. Network Monitoring Port
   4. Spanning Tree Operation
   5. IP Configuration
   6. SNMP Community Names
   7. IP Authorized Managers
   8. VLAN Menu...
   0. Return to Main Menu...

Configures IP service for switch management.
To select menu item, press item number, or highlight item and press <Enter>.
```

Obr. 3.2: Konfigurační menu switche HP2626

V položce **5. IP Configuration** zprovozníme přístup k přepínači pomocí webového rozhraní (obr. 3.4). A to tak, že položku **IP Config [DHCP/Bootp]** nastavíme na **Manual** a přiřadíme switchi IP adresu a masku sítě (obr. 3.3). IP adresa a maska musí být kompatibilní se zbytkem sítě. Zadáme-li tuto adresu do prohlížeče, zobrazí se webové konfiguračního rozhraní, které je více přehlednější než konfigurační menu terminálu, a hlavně nám umožní vzdálenou zprávu přepínače z libovolného místa internetové sítě.

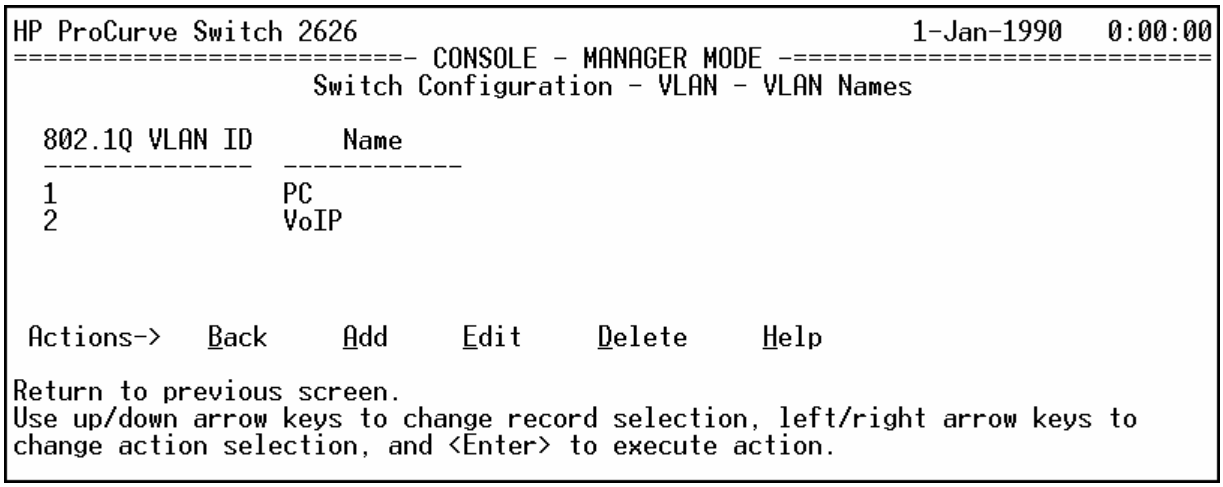
```
IP Config [DHCP/Bootp] : Manual
IP Address  : 147.229.148.120
Subnet Mask : 255.255.254.0
```

Obr. 3.3: Nastavení IP adresy a masky sítě



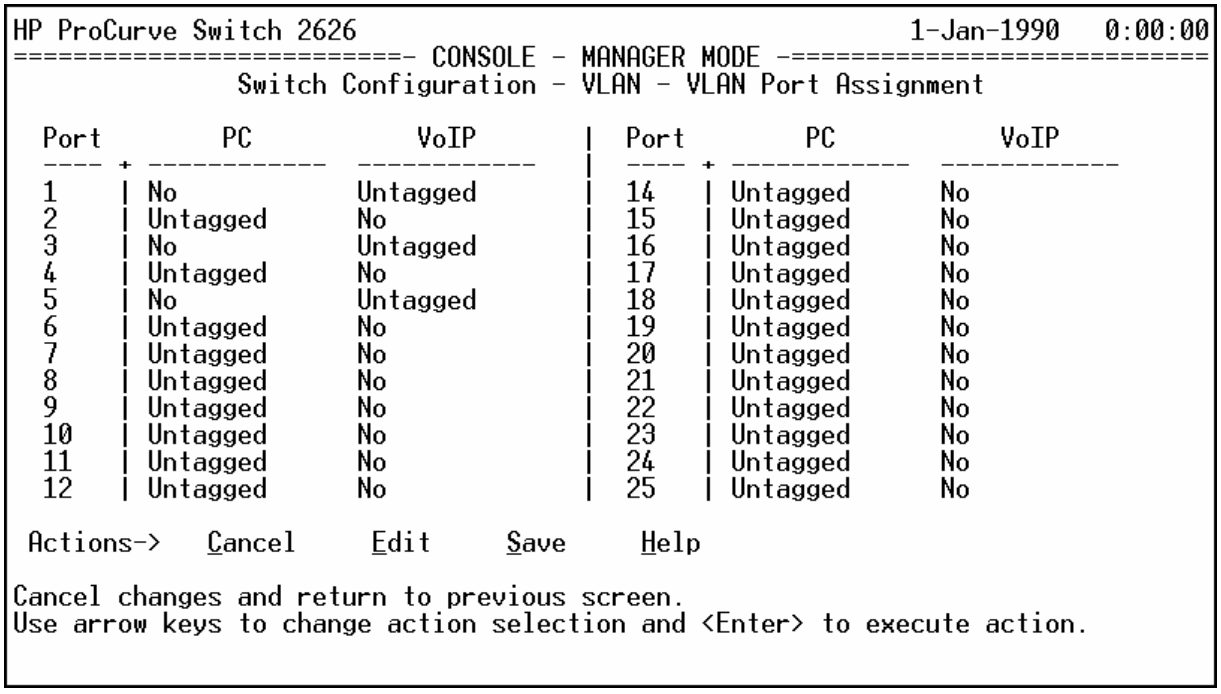
Obr. 3.4: Webové rozhraní HP2626

V dalším kroku vytvoříme dvě virtuální počítačové sítě pro PC a IP telefony (Main Menu/Switch Configuration/VLAN/VLAN Names) příkazem **Add** zadáme **VLAN ID** (1 a 2) a **Name** (PC a VoIP) podle obr.3.5.



Obr. 3.5: Vytvoření potřebných VLAN

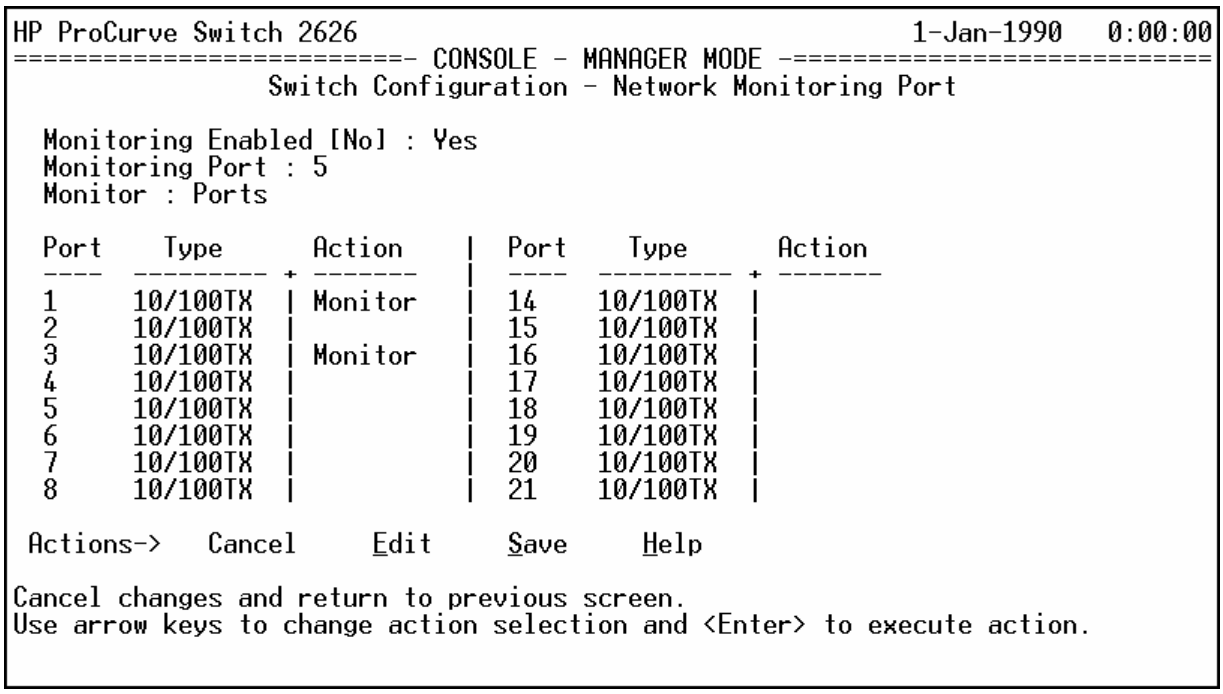
Do takto vytvořených virtuálních sítí přiřadíte jednotlivé porty (/VLAN/VLAN Port Assignment – obr. 3.5). Ve virtuální síti **PC** ponecháme všechny porty kromě portů 1, 3, 5 (IP telefony a monitorovací stanice) a hlavního portu 26. Tyto přiřadíme VLAN s názvem **VoIP**.



Obr. 3.6: Porty přiřazené jednotlivým VLAN

Na závěr nastavíme monitorování portů (Main Menu/Switch Configuration/Network Monitoring Port) dle obr. 3.6. Povolíme funkci monitorování (**Yes**). Zvolíme port, na který chceme přeposílat datový tok (v našem případě port číslo **5**), kde je připojeno monitorovací PC a vybereme porty zařízení, jejichž pakety budeme zachytávat

(IP telefony připojené na porty 1 a 3). V tuto chvíli je směrovač nastaven dle požadavků a připraven k simulaci a analýze.



Obr. 3.7: Nastavení monitorování portů

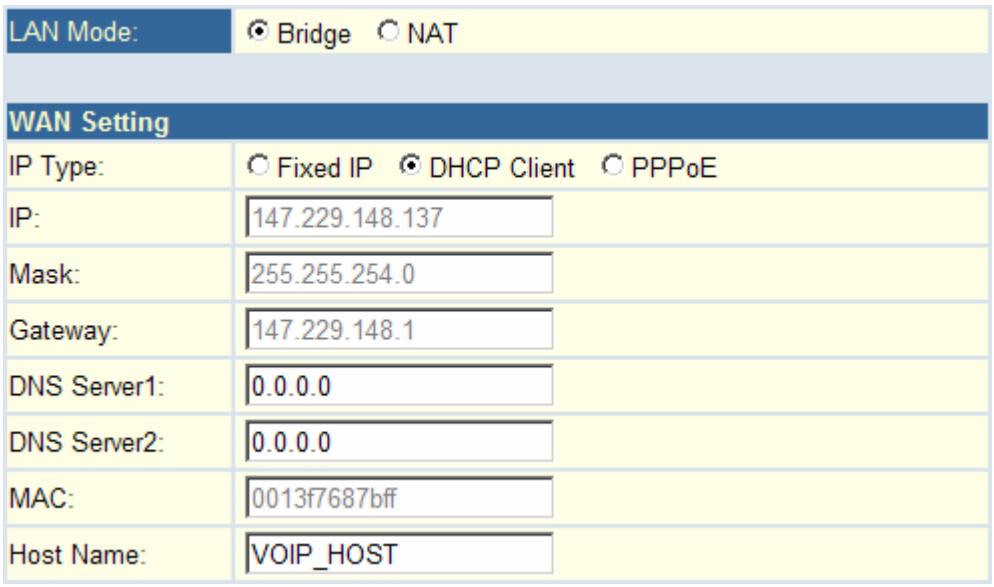
3.2 IP telefony

IP telefon od firmy SMC je hardwarově řešený klient pro telefonii typu VoIP. Je to telefonní přístroj, který komunikuje prostřednictvím svého rozhraní protokolem IP. Rozhraní IP telefonu je opatřeno dvěma konektory RJ-45. Jeden slouží k přímému připojení do počítačové sítě (označený WAN) a přes druhý může být do sítě připojeno PC (označení LAN). Telefon je vybaven také konektorem pro připojení vnějšího napájení elektrickou sítí.

3.2.1 Nastaveni telefonů

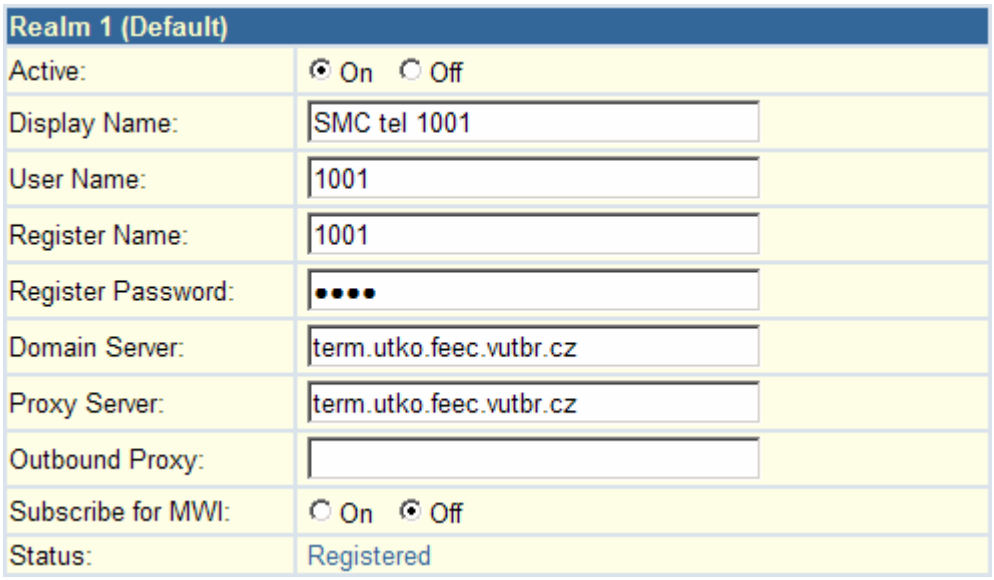
Pro připojení se k IP telefonu použijeme webový prohlížeč. Zde zadáme IP adresu telefonu, jenž chceme konfigurovat, a číslo portu ":9999" za tuto adresu. V našem případě **147.229.148.135:9999** pro první telefon a **147.229.148.137:9999** pro druhý. Zobrazí se úvodní okno, kde je potřeba zadat přihlašovací údaje **Username** a **Password** (možné zjistit u pověřené osoby).

V položce **Network/WAN Setting** (obr. 3.8) zatrhneme v řádku **LAN Mode** funkci **Bridge**. V řádku **IP type** zatrhneme **DHCP Client** – IP adresu bude telefonu automaticky přidělovat DHCP server.



Obr. 3.8: Nastavení automatického přidělování IP adresy telefonu

V dalším nastavení (položka **SIP Petting/Service Domain**) je potřeba telefony přihlásit k ústředně, která bude spojovat jejich vzájemné hovory. Nastavení provedeme podle obr. 3.9. Konfigurace pro druhý telefon bude stejná, pouze hodnotu **1001** změníme na **1002**. **Display Name** je název, který se objeví na displeji příslušného telefonu. **User Name** je jméno telefonu (můžeme zvolit libovolně). **Registered Name** a **Registered Password** je název a heslo, pod kterým budeme telefon registrovat k ústředně. Do kolonky **Domain** a **Proxy Server** zadáme adresu severu, na kterém je nainstalována softwarová ústředna spravující telefony (v našem případě **term.utko.feec.vutr.cz**).



Obr. 3.9: Nastavení IP telefonu pro registraci k ústředně

3.3 VoIP ústředna

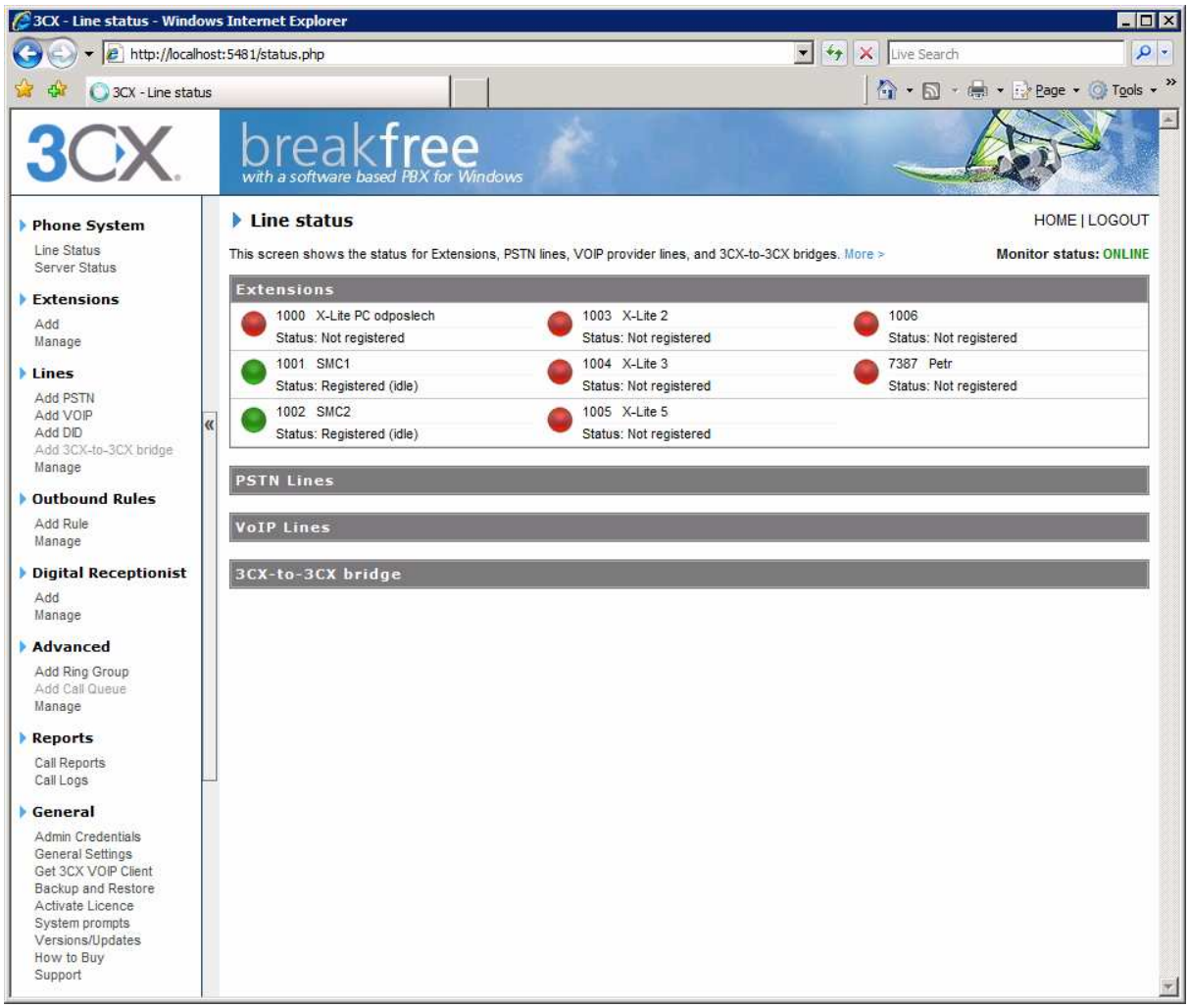
Telefonní systém 3CX pro Windows je IP PBX na bázi software a nahrazuje tradiční hardwarové či automatické pobočkové ústředny. Je založen na využití standardu SIP – snadněji se tedy spravuje a umožňuje uživateli používat jakýkoli telefon na bázi SIP (softwarový nebo hardwarový) [16].

3.3.1 Výhody IP PBX na bázi software:

- Nevyžaduje zvláštní telefonní rozvody – využívá počítačovou síť
- Snadná konfigurace a správa prostřednictvím webového konfiguračního rozhraní
- IP PBX na bázi software je mnohem levnější než hardwarové či automatické pobočkové ústředny (3CX v základní verzi dokonce freeware)
- Uživatelé mohou měnit pracovní místa bez nutnosti provádět změny v rozvodech nebo v konfiguraci IP PBX
- Umožňuje připojení většiny hardwarových telefonů na bázi SIP; není nutno vázat se na jednoho dodavatele
- Příjem hovorů nebo telefonie prostřednictvím standardní linky PSTN
- Snížení nákladů za volání při využití služeb SIP VoIP nebo WAN

3.3.2 Zásadní funkce systému 3CX:

- Kompletní telefonický systém – Poskytuje přepojování hovorů, směrování a čekání
- Rozšiřitelnost – Zaručuje neomezené množství linek a přípojů
- Webová konfigurace a ukazatel stavu – Snadné řízení telefonického systému
- Sjednocené zprávy – Přijímání hlasové pošty přes e-mail
- Automatické přiřazování (např. 1 pro obchod, 2 pro podporu, atd.)



Obr. 3.10: Pohled na konfigurační menu 3CX softwarové ústředny

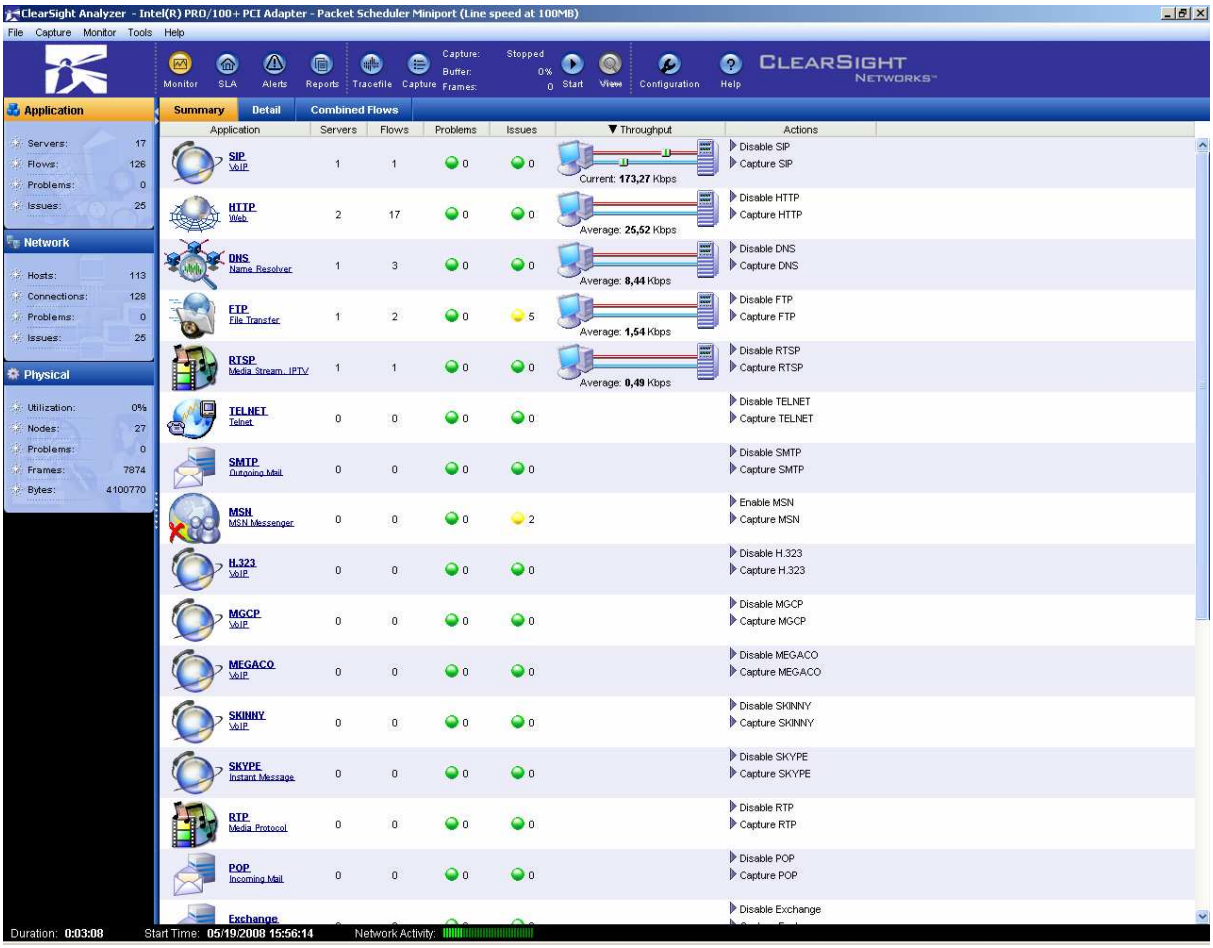
3.4 ClearSight Analyzer

ClearSight je softwarový protokolový analyzátor využívající hardwarových prostředků PC a síťové karty s příslušným Ethernetovým rozhraním 10/100/1000 MB/s. K dispozici je také výkonné kompletní HW/SW řešení pro Ethernet. Grafické uživatelské prostředí nabízí řadu nástrojů pro rychlé a efektivní řešení problémů nejrůznějších aplikací z oblasti internetu, emailových služeb, databázových systémů a multimediálních přenosů hlasu a videa.

Analyzátor poskytuje možnost monitoringu protokolů jednotlivých aplikací v reálném čase, detailní sledování průběhu jednotlivých spojení ve formě komunikačního diagramu včetně časových relací. Uživatelské prostředí je zobrazeno v přehledném vrstvovém stylu, kde je možno kliknutím na ikony a prvky otevřít detailnější popis.

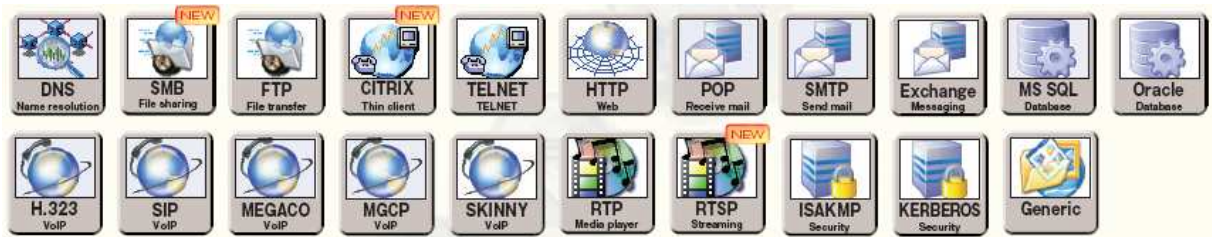
Systém ClearSight umožňuje zobrazení provozu v reálném čase pro okamžitý přehled nad obsahem komunikačního toku. U aplikací jako jsou Internet, FTP, Telnet, e-mail,

databáze a VoIP je možné přesně zrekonstruovat obsah komunikace z paketů procházejících sítí v reálném čase nebo z předem zachycených a uložených dat [17].



Obr. 3.11: Úvodní okno analyzátoru

3.4.1 Aplikace podporované analyzátorem ClearSight:



Obr. 3.12: ClearSigh analyzátorem podporované aplikace

VoIP – ClearSight provádí detailní analýzu provozu jak z pohledu sestavování spojování, tak určování kvality hlasu. Podporuje analýzu protokolů jako jsou SIP, H.323, Cisco SKINNY, MGCP, MEGACO a RTSP. Dále podporuje JPEG (411, 422, 111), H.263 Mode A, Mode B, MPEG4 kodeky.

Proces výměn paketů mezi více uzly včetně telefonních terminálů a relay serverů je automaticky přiřazen k danému hovoru a následně je celá komunikace zobrazena ve formě příčkového diagramu (ladder view). Celý průběh spojení, od sestavení po ukončení, je možno sledovat v reálném čase nebo vyvolat z uložených dat.

Hlášení QoS příslušného VoIP hovoru může být jednoduše vygenerováno kliknutím na určenou položku.

Web – HTTP

E-mail - POP, SMTP, Exchange

Databáze - MS SQL, Oracle. ClearSight nabízí detailní analýzu provozu Klient-Server pro potřeby databázových aplikací, užitých v páteřních podnikových systémech a při různých obchodních aktivitách.

Bezpečnost - ISAKMP, KERBEROS

Sdílení souborů - SMB, FTP

Thin Client/Terminal - CITRIX, TELNET

3.4.2 ClearSight Reporter

Reporter je nástroj pro sběr statistik o jednotlivých aplikacích, serverech atd. a jejich dalším použití pro automatické vytváření reportů. Reporty mohou být založeny na sledování v reálném čase nebo na datech získaných z předchozích monitorování.

Reporty mohou být vytištěny ve stejném formátu v jakém se objevují na obrazovce nebo mohou být exportovány do PDF, HTML nebo RTF formátu. Je také možno vygenerovat speciální uživatelsky definované reporty, které zahrnují statistiky o více prvcích dohromady.

Navíc Reporter umožňuje monitorovat vývoj stavu aplikací, sítě a dalších prvků a shromažďovat data získaná v reálném čase v databázi. Shromažďováním statistik po delší dobu umožňuje uživateli vytvářet reporty dlouhodobějšího charakteru a tím monitorovat vývoj aplikací, sítě aj. Časový úsek může být nastaven na jednotlivé dny, týdny nebo specifikován manuálně, čímž se zjednodušuje proces generace periodických reportů [17].

3.5 NetTool Serie II

NetTool je hardwarový analyzátor, který umožní snadné monitorování sítě a řešení problémů s konektivitou. Zapojuje se přímo do sítě mezi jednotlivá zařízení a nebo na

konec. NetTool kombinuje výkonné diagnostiky NetProve, inline Gigabit vision, digitální technologii IntelliTone a testování konfigurace sítě, IP telefonů a počítačů do jednoho přenosného přístroje.

3.5.1 Základní vlastnosti

Zde jsou popsány základní funkce analyzátoru NetTool [18]:

Monitorování a autentizace NetSecure – funkce Port Monitor pro rozlišení neočekávaného provozu v síti, který je zapříčiněn škodlivými aplikacemi (spyware atd.).

NetProve diagnostiky – určí příčiny problémů zařízení a aplikací s konektivitou.

Inline Gigabit vision – řeší rychle síťové problémy díky účinnému inline pohledu na 10/100/Gigabitový provoz mezi přepínači, počítači, IP telefony a jinými zařízeními.

Řešení problémů s VoIP – inline připojením je možné monitorovat VoIP hovory, takže lze rychle diagnostikovat boot IP telefonů, problémy s kontrolou hovorů a shromažďovat data pro klíčové statistiky kvality hovorů.

PoE měření – ověření funkčnosti PoE systémů a případné řešení problémů PoE zařízení.

Dostupné síťové zdroje – možnost zjištění MAC a IP adresy, podsítě a služby nabízené aktivními servery, routery a tiskárnami.

Digitální vyhledávání pomocí IntelliTone – rychle a s jistotou lokalizuje kabely na aktivní síti

4. OPTIMALIZACE SÍŤOVÉHO PROVOZU - VZOROVÝ PROTOKOL

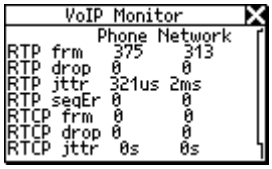
Přepínač jen nakonfigurován dle požadavků uvedených v zadání úlohy (kap. 2.2). Jak již bylo uvedeno výše, měření datových toků v síti bude probíhat zejména v reálném čase. ClearSight analyzátor monitoruje síťový provoz ihned po spuštění programu. Naskytne se tak pohled na veškerý provoz na síťovém adaptéru. V online sledování program zobrazuje pouze komunikaci jednotlivých protokolů a jim odpovídající komunikační diagramy. Skutečná data nejsou ukládána z důvodu velké kapacity. Chceme-li však přímo zjistit o jaká data šlo, je potřeba nastavit a spustit zachytávání rámců (viz. kap. 5).

4.1 Odposlech hovoru mezi IP telefony

Na monitorovací stanici (zapojení dle obr. 2.1) spustíme program ClearSight, kde v položce **Capture** nastavíme a spustíme zachytávaní dat. Můžeme také nastavit filtrování pro protokoly SIP a RTP, které slouží k sestavení spojení a k přenosu hovoru. NetTool analyzátor zapojíme inline mezi jeden z IP telefonů. Příkazem **Auto Test** provedeme diagnostiku zapojení. Detailnější pohled na zapojení telefonu je pod položkou Log VoIP (obr. 4.1).

Obr. 4.1: Informace o připojeném IP telefonu

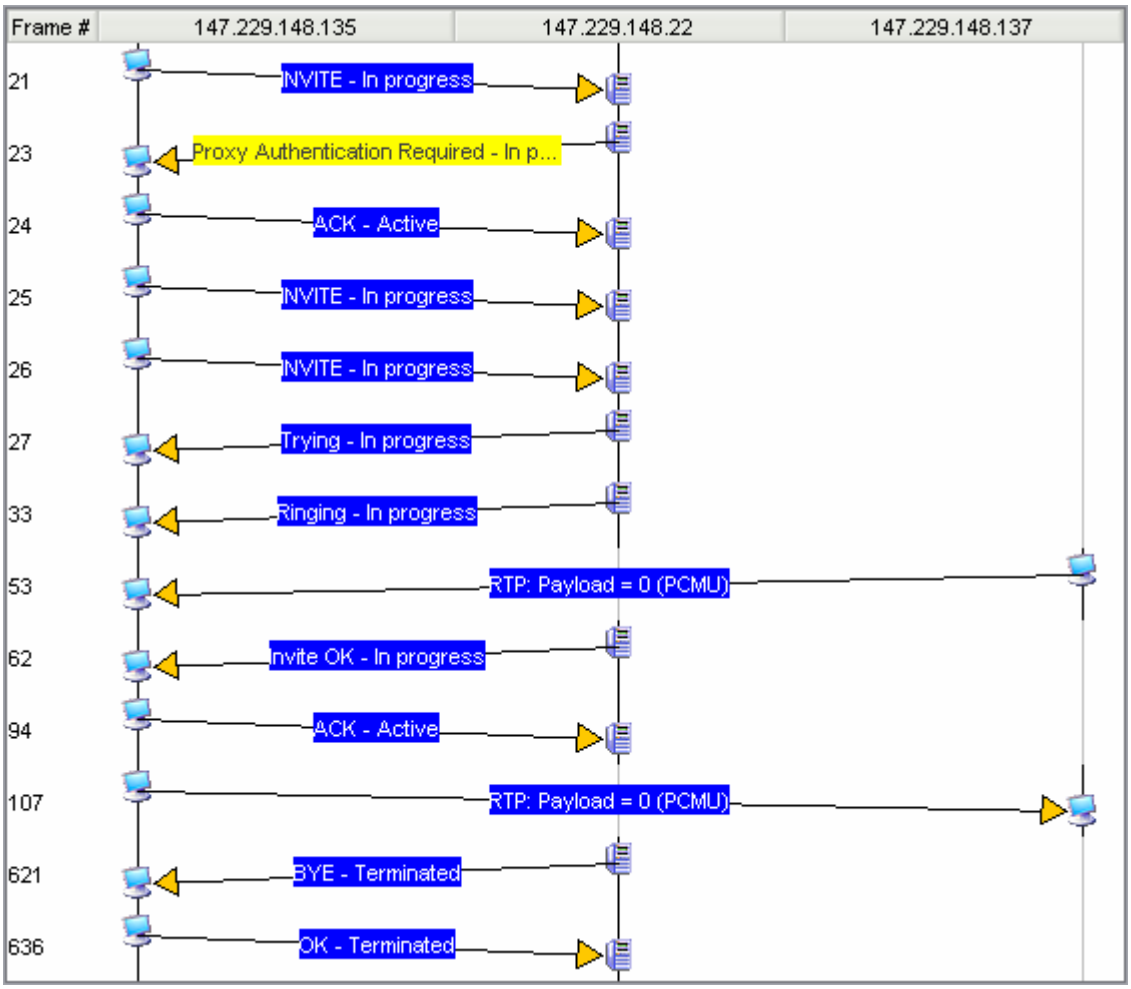
Uskutečníme několik krátkých hovorů mezi IP telefony. Během nich můžeme na NT sledovat pod položkou VoIP Monitor přenesené rámce, zpoždění mezi telefony a případné chyby v přenosu (obr. 4.2). Po ukončení všech hovorů vypneme v programu ClearSight zachytávání rámců a zobrazíme si naměřené výsledky.



Obr. 4.1: Monitorování hovoru na NT

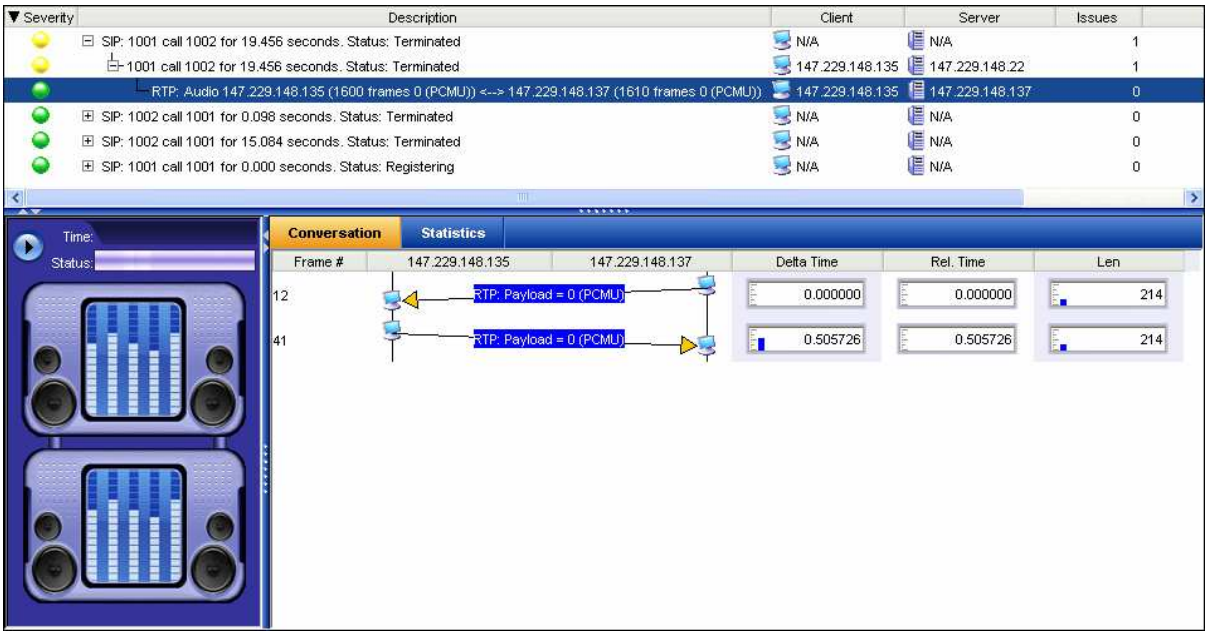
4.1.1 Analýza zachyceného hovoru

Na obr. 4.2 je znázorněn průběh komunikace mezi IP telefonem (.135) a softwarovou ústřednou (.22) při uskutečnění telefonního hovoru. Můžeme vidět přihlášení telefonu k ústředně, navazovaní spojení, vyzvánění, průběh hovoru a ukončení hovoru. Samotného průběhu hovoru (protokol RTP) se již ústředna neúčastní, telefony jsou ve spojení pouze mezi sebou.



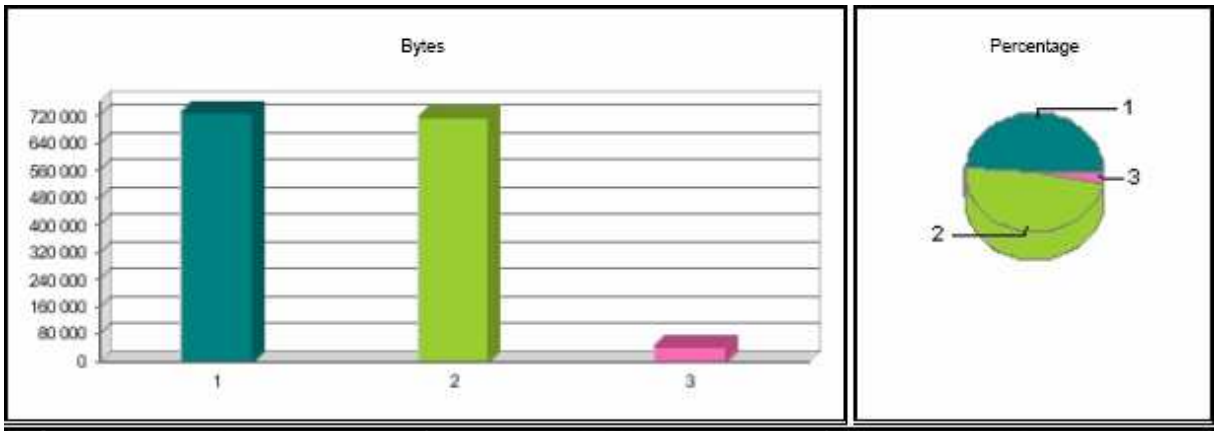
Obr. 4.2: Průběh komunikace při uskutečni hovoru mezi IP telefony

Na obr. 4.3 můžeme sledovat detailnější pohledy na jednotlivé hovory. Každý řádek představuje jedno realizované telefonní spojení. Po rozkliknutí řádku vidíme hierarchicky průběh sestavení spojení. V řádku RTP se naskytne možnost přehrát si zachycený telefonní hovor přímo v programu. Spustíme ho tlačítkem Play (➢).



Obr. 4.3: Ukázka možnosti poslechu zaznamenaného hovoru

Výstupem tohoto měření jsou jednotlivé reporty exportované z analyzátorů. Na obr. 4.4 můžeme vidět počet přenesených bytů jednotlivých zařízení. Zelené sloupce představují IP telefony, mezi kterými probíhá hlavní datový tok protokolu RTP (viz. také obr. 4.5). Růžový sloupec zobracuje data přenesená ústřednou (serverem). Je zde vidět velmi malý datový tok v porovnání s IP telefony. Protože ústředna zajišťuje komunikaci mezi IP telefony a sestavení spojení (protokol SIP), ale hovoru se již neúčastní, datový tok probíhá přímo mezi IP telefony (Obr. 4.2).



	Address	Total Frames	Total Bytes
1	147.229.148.137	3 249	725 909
2	147.229.148.135	3 237	716 666
3	147.229.148.22	66	43 015

Obr. 4.4: Grafy zobrazující objem přenesených bytů mezi IP telefony a ústřednou

Na obr. 4.5 je porovnání využitých protokolů RTP a SIP. Popsanou situaci dokazují grafy. Příloha 1 je výstupem NT analyzátoru, jsou zde uvedeny informace o zařízeních, mezi které jsme NT připojili. Např.: využívané internetové protokoly, IP adresy DNS a DHCP serveru, výstupní brány atd. V části VoIP Monitor je uvedeno množství přenesených rámců a zpoždění během hovoru.

	Application	Bytes	Frames
1	RTP	699 780	3 210
2	SIP	43 015	66

Obr. 4.5: Porovnání přenesených bytů během hovoru protokoly RTP a SIP

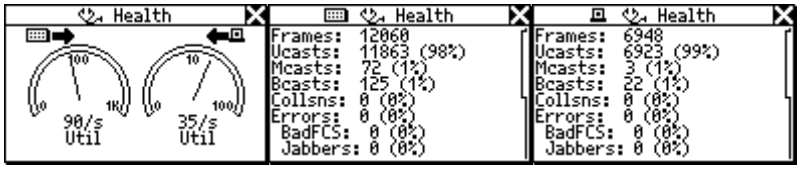
4.2 Ochrana sítě proti neoprávněnému přístupu

Současná doba klade velký důraz na zabezpečení počítačových sítí. Platí, že čím bezpečnější síť chceme mít, tím musíme použít složitější a také nákladnější technologie. Jeden z možných způsobů, jak zabezpečit vytvořenou počítačovou síť, je aktivovat na přepínači seznam povolených MAC adres. Bude-li, k přepínači připojeno zařízení jehož MAC adresa není zahrnuta ve zmíněném seznamu, nebude přepínačem vůbec obsluhováno. Bohužel i MAC adresa se dá v počítači snadno zfalšovat. Proto je vhodné pro vyšší úroveň zabezpečení nevyužívané porty přepínače blokovat. Útočník by se do sítě musel připojit místo zařízení, které má povolenu komunikaci se sítí a také by musel znát jeho MAC adresu. Pro laboratorní využití výše popsané zabezpečení dostačuje. Uvažujeme-li o školní síti jako jednom celku, je vhodné použít vyšší úroveň zabezpečení (např.: autentizační protokoly). Pro zabezpečení hovoru se často využívá technologie Voice VPN, která podobně jako v běžných VPN sítích aplikuje šifrování s použitím technologie IPSec na datový tok.

4.3 Monitorování provozu v počítačové síti

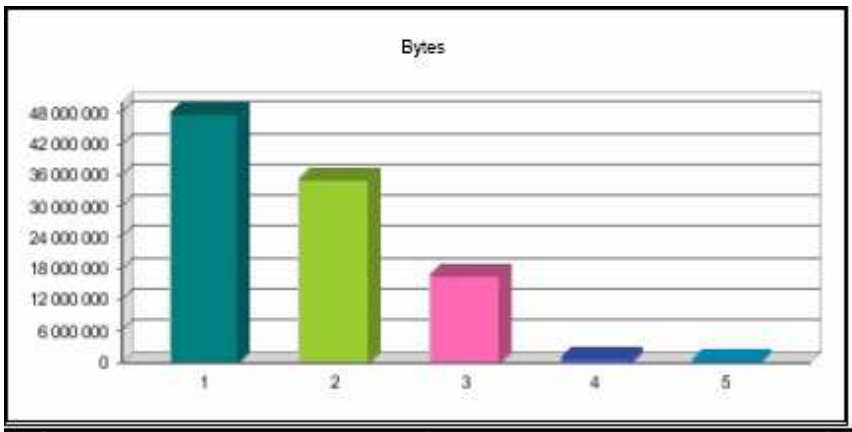
Mezi jeden z počítačů v laboratoři, který je připojen k VLAN1 (obr. 2.1), a přepínač zapojíme NetTool analyzátor a spustíme program ClearSight. Nastavení obou analyzátorů je obdobné jak již bylo popsáno v kap. 4.1 pouze s tím rozdílem, že se zaměříme na monitorování jiných protokolů. Budeme sledovat využití sítě běžným uživatelem, jako jsou návštěvy nejrůznějších internetových stránek (protokol HTTP), posílání a příjem emailů (protokol POP a SMTP), sledování internetových videí (protokol RTSP) a stahování (nahrávání) dat z FTP serveru či používaní některého z IM komunikátorů (ICQ, Skype, Jabber).

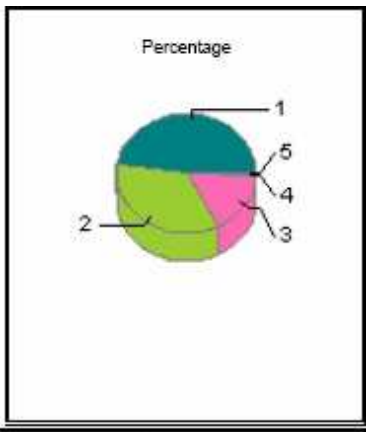
Během těchto úkonů můžeme na NT monitorovat datový tok. Na obr. 4.6 je uveden příklad analýzy dat (aktuální přenosová rychlost toku dat odeslaných ze sítě a PC, podrobné zobrazení typu rámců mezi PC a sítí).



Obr. 4.6: Rychlost a počet přenesených rámců mezi PC a sítí

Po zachycení dat analyzátorem ClearSight můžeme zpětně vystopovat veškerou komunikaci uživatele s okolní sítí. Např. u protokolu FTP snadno zjistíme jméno a heslo, které bylo použito k přihlášení se na server. Ale také přímou adresářovou strukturu serveru, tak jak ji viděl uživatel a soubory, které na server nahrál či stáhnul do svého počítače. Tyto jednotlivé kroky jsou vyobrazeny u každého spojení v přehledném komunikačním diagramu (obr. 5.5). Informace o měření je možné zaznamenat v jednotlivých reportech podle nejrůznějších kritérií. Jeden z mnoha možných reportů je na obr. 4.7. Vyobrazuje pět nejpoužívanějších protokolů v aplikační vrstvě dle objemu přenesených dat.





	Application	Bytes	Frames
1	FTP	47 702 528	42 251
2	RTSP	34 964 153	30 022
3	Others	16 521 442	23 057
4	HTTP	677 043	1 104
5	CITRIX	23 611	52

Obr. 4.7: Zobrazující použité protokoly dle objemu přenesených bytů

Celkový výsledek měření analyzátorem NetTool je uveden v závěrečné zprávě v podobě reportu exportovaného z analyzátoru pomocí obslužného programu (příloha 2). Report je rozdělen na čtyři hlavní části – **Host**, **Network**, **Protocols** a **Key Device**. V části **Host** jsou informace o připojeném PC, charakteristika ethernetového kabelu mezi NT a PC (délka, přenosová rychlost, duplex), použité adresy (IP adresa, maska sítě, MAC adresa, síťová skupina), využívané síťové servery a jejich IP adresy (DHCP, DNS, WINS, výchozí brána), statistika přenesených rámců z počítače směrem do sítě (počet, typ). **Network** zahrnuje hlavní informace o síti, k níž je klient připojen, charakteristiku ethernetového kabelu mezi NT a sítí, síťové IP adresy a statistiku přenesených rámců ze sítě směrem do počítače. Část **Protocols** určuje, které z uvedených protokolů jsou sítí podporovány. Poslední **Key Device** určuje hlavní zařízení v počítačové síti (jednotlivé servery a routery) a jim odpovídající IP adresy.

5. MANUÁL K ANALYZÁTORU CLEARSIGHT

Seznámení se s obsluhou síťového analyzátoru **ClearSight Analyzer**. V následujících odstavcích jsou popsány nejdůležitější nastavení, použití nejrůznějších statistik pro monitorování, analýzu a následné odhalování chybových stavů při provozu hlasových a datových služeb v počítačových sítích založených na IP protokolu.

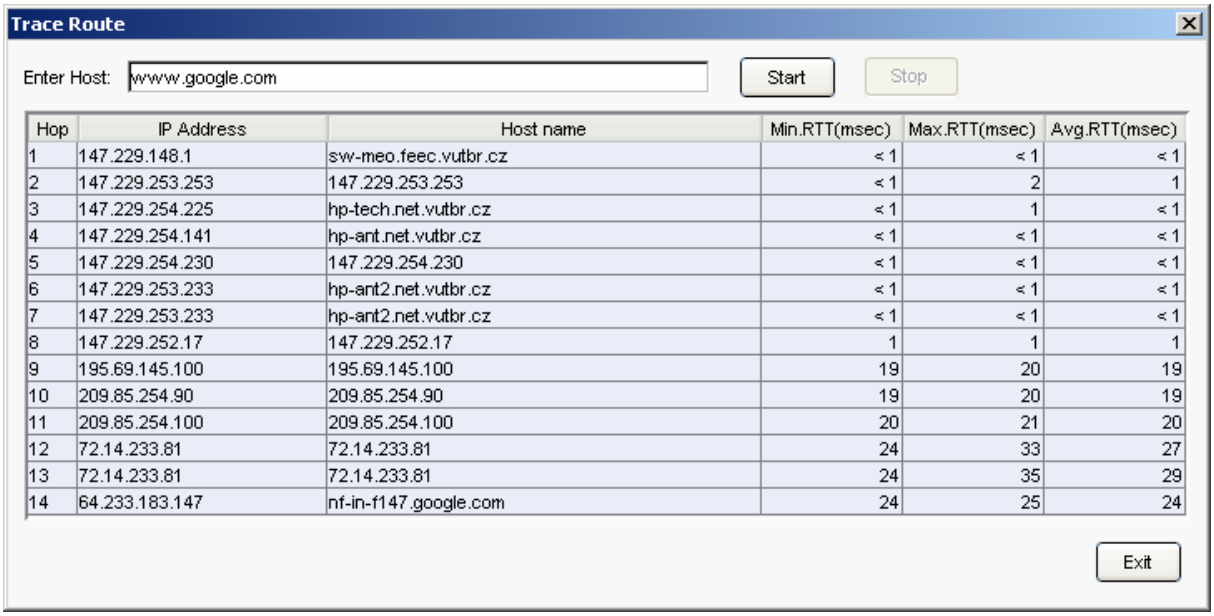
5.1 Popis jednotlivých položek hlavního panelu

File – otevření, uložení analyzované relace, nastavení tisku a tisk reportů, výběr síťového adapteru používaného k měření, konec programu

Capture – spuštění, zastavení či zobrazení výsledků zachycených rámců

Monitor – reset celého analyzátoru (vymaže veškerá dosud zachycená data v reálném čase), funkce zachycení vybrané obrazovky v podobě obrázků

Tools – zde se nachází funkce Trace Route obr. 5.1 (zaznamená přes jaké uzly putují data od klienta k požadovanému severu a zpoždění v každém uzlu).



Hop	IP Address	Host name	Min.RTT(msec)	Max.RTT(msec)	Avg.RTT(msec)
1	147.229.148.1	sw-meo.feec.vutbr.cz	< 1	< 1	< 1
2	147.229.253.253	147.229.253.253	< 1	2	1
3	147.229.254.225	hp-tech.net.vutbr.cz	< 1	1	< 1
4	147.229.254.141	hp-ant.net.vutbr.cz	< 1	< 1	< 1
5	147.229.254.230	147.229.254.230	< 1	< 1	< 1
6	147.229.253.233	hp-ant2.net.vutbr.cz	< 1	< 1	< 1
7	147.229.253.233	hp-ant2.net.vutbr.cz	< 1	< 1	< 1
8	147.229.252.17	147.229.252.17	1	1	1
9	195.69.145.100	195.69.145.100	19	20	19
10	209.85.254.90	209.85.254.90	19	20	19
11	209.85.254.100	209.85.254.100	20	21	20
12	72.14.233.81	72.14.233.81	24	33	27
13	72.14.233.81	72.14.233.81	24	35	29
14	64.233.183.147	nf-in-f147.google.com	24	25	24

Obr. 5.1: Záznam cesty dat sítí pomocí funkce Trace Route

5.1.1 Panel nástrojů

Obr. 5.2: Panel nástrojů programu ClearSight

Monitor	Zobrazení nabídky pro monitorování v reálném čase
SLA	Service Level Agreement monitoring pro ověření kvality služeb
Alerts	Zobrazení okna s výstrahami a problémy s konektivitou
Reports	Zobrazení nabídky pro vytváření reportů
Tracefile	Nabídka pro práci s již uloženými analýzami
Capture	Zobrazení okna pro nastavení parametrů zachytávání
Start	Spuštění zachytávání dat
View	Zobrazení právě zachycených rámců uložených v bufferu
Configuration	Konfigurace analyzátoru nastavení filtrů a varování
Help	Přístup k online nápovědě ClearSight Analyzátoru

ClearSight analyzátor využívá vrstvový způsob uživatelského rozhraní, což nám umožní dostat se pomocí kliknutí od úplného souhrnu informací o probíhající komunikaci, k detailnějšímu pohledu na konkrétní protokol, či přímo vidět pozici vybraného bytu v rámci. Data jsou v ClearSight analyzátoru organizována ve třech hlavních vrstvách (obr. 5.3): aplikační (zobrazení protokolů jednotlivých aplikací; pohled na datové toky mezi aplikacemi a navštívené servery), síťová (zobrazení protokolů síťové a transportní vrstvy; hostitele, přes které probíhá komunikace; počet či druh realizovaných spojení) a vrstvy fyzické (záznam objemu přenesených dat a rámců; pohled na uzly, které umožnily propojení zařízení).

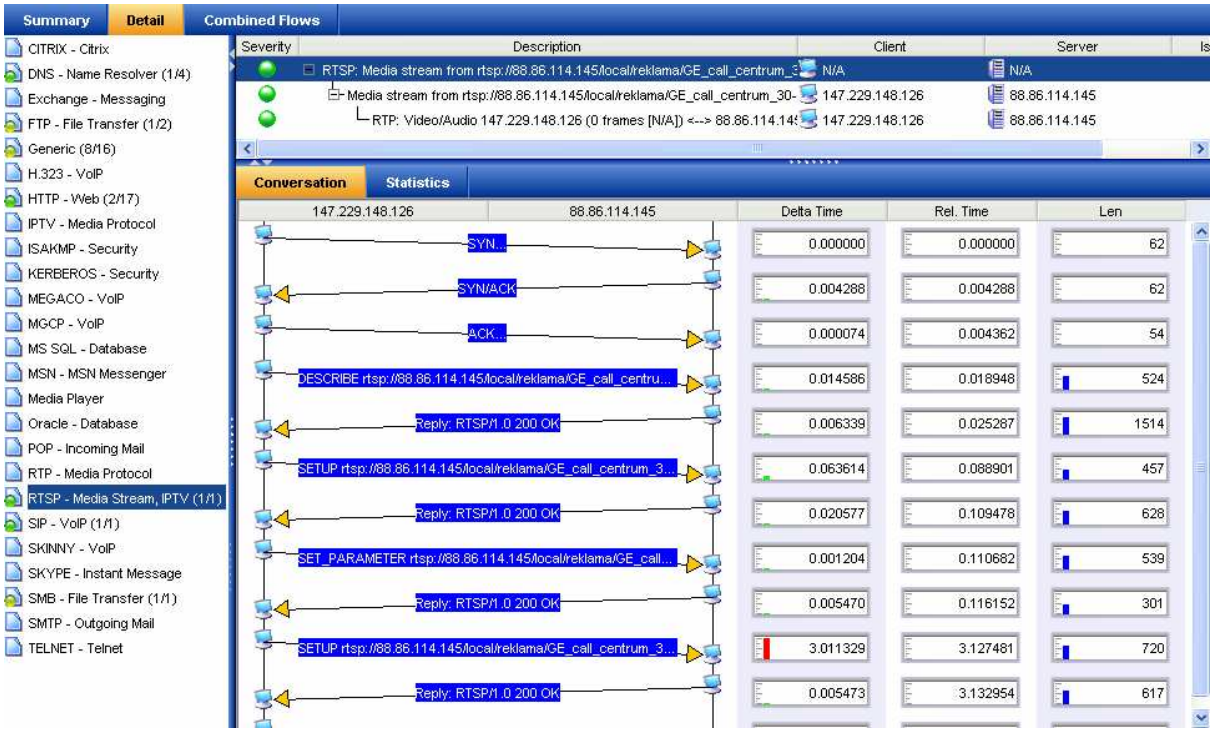
Obr. 5.3: Porovnání vrstev modelu OSI a ClearSight

5.2 Popis jednotlivých oken

SUMMARY toto okno (obr. 5.4) ukazuje souhrnný pohled na veškeré protokoly a jejich aktivitu v reálném čase. Můžeme jednotlivé protokoly vyřadit a sledovat tak jen námi definované provozy.

Obr. 5.4: Pohled na monitorovaný provoz v síti v reálném čase

DETAIL tato položka nám umožní podrobnější pohled na jednotlivé protokoly a komunikační diagramy. Okno s diagramem (obr. 5.5) můžeme přepnout na **Statistics** a zobrazit si tak statistické údaje vybraného přenosu. Při monitoringu v reálem čase se pouze monitoruje síťový provoz a vytváří komunikační diagramy. Chceme-li nahlédnou přímo na konkrétní data, je potřeba nejdřív nastavit zachytávání rámců **Capture** a spustit tlačítkem **Start**. Poté, co zachytíme potřebná data, stačí přejít tlačítkem **Wiew** k jejich vyhodnocení. Objeví se nové tlačítko **Decode** pro podrobný pohled na zachycené rámce viz. dále.



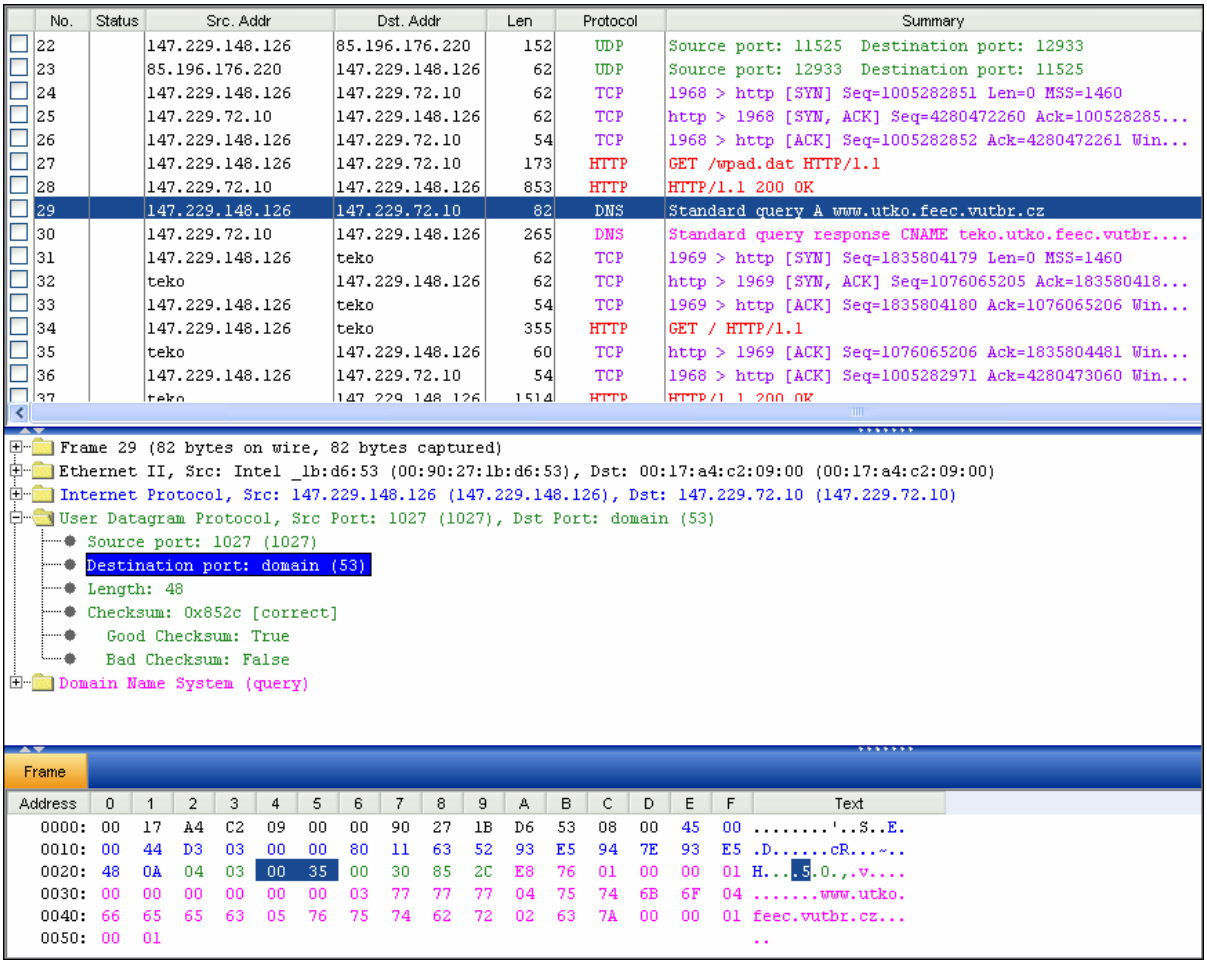
Obr. 5.5: Detailnější pohled na monitorovaný provoz v síti v reálném čase

DECODE v prvním okně (obr. 5.6) jsou vidět jednotlivé rámce po sobě jdoucí. Je zde pořadové číslo rámce, zdrojová a cílová adresa, délka (velikost) rámce, použitý protokol, shrnutí informací o daném rámci, skutečný čas (uplynulá doba od prvního paketu), průměrný čas (uplynulá doba od předchozího paketu) a absolutní čas (datum a aktuální čas).

V dalším okně je vidět detailnější popis konkrétního rámce dle jednotlivých vrstev. Opět další podrobnější informace o rámci (po rozkliknuti můžeme vidět pořadové číslo, skutečný a průměrný čas, velikost v bytech a informaci o využitých protokolech v rámci). Na dalších řádcích následují jednotlivé protokoly: Ethernetový, IP, UDP, DNS. Při kliknutí

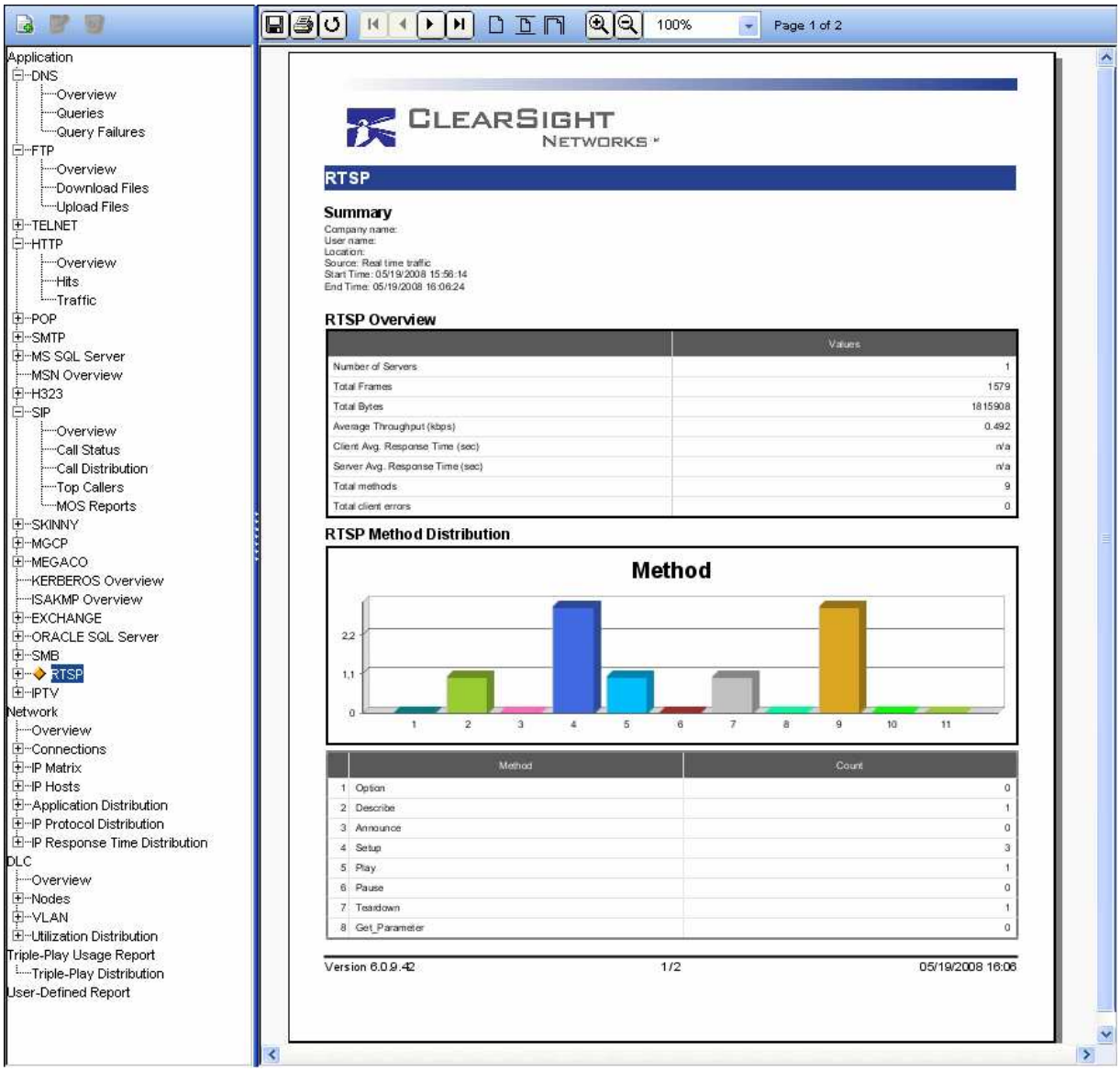
na libovolný řádek se ve třetím okně, zvýrazní právě ty byty, které odpovídají tomuto řádku.

Poslední třetí okno zobrazuje jednotlivé byty tak, jak jsou po sobě přenášeny sítí. Pole jsou barevně rozlišena podle toho, do jaké vrstvy daný byte patří.



Obr. 5.6: Pohled na po sobě jdoucí rámce a jejich detaily

REPORTS v této položce (obr. 5.7) je možné vytvořit jednotlivé zprávy o analyzovaných datech. Tyto reporty nám poslouží jako přehledný výstupní protokol, který můžeme použít k dalšímu zpracování. V levém sloupci vybereme protokol, který nás zajímá a můžeme si také nadefinovat vlastní report pro více námi vybraných protokolů. Napravo se objeví náhled na příslušný report, který je připraven přímo k tisku či uložení na pevný disk ve zvoleném formátu (PDF, HTML, RTF).



Obr. 5.7: Náhled na vytvořený report o měření

6. MANUÁL PŘÍSTROJE NETTOOL SERIES II

6.1 Popis jednotlivých tlačítek a indikátorů NT

Jak je vidět na obr. 6.1 k ovládání analyzátoru slouží jen několik tlačítek. Práce s přístrojem je velice snadná a zvládne ji opravdu každý uživatel. Zelené tlačítko slouží k zapnutí a vypnutí přístroje, navigační tlačítka k pohybu v menu a tlačítko **Select** pro výběr.

Obr. 6.1: Popis tlačítek a indikátorů NT analyzátoru

Indikátor rychlosti připojené linky svítí zeleně pro rychlost 10 MB/s, modře pro 100 MB/s a bíle pro 1GB/s. Indikace chyby a kolize se rozsvítí červeně, byla-li detekována chyba v síti a žlutě nastane-li kolize. Indikátor pro zatíženi daného portu má 3 stavy:

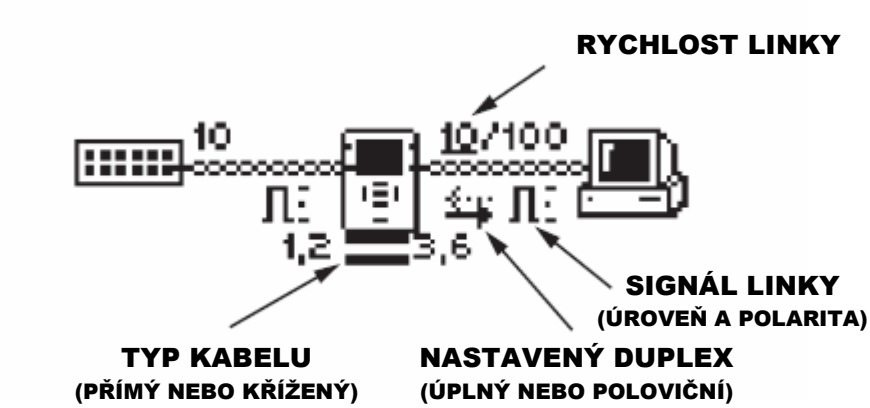
zelený, je-li zatížení linky pod 50%; žlutý určuje zatížení mezi 50 a 90%; červený, překročí-li datový toky 90% možného využití linky. Indikace napájení svítí, když je NT připojen přes nabíjecí adaptér do elektrické sítě. Indikátor PoE se rozsvítí, když tester pozná že je na lince provozováno napájení pomocí ethernetové linky.

6.2 Spuštění:

- Připojte NetTool Series II do počítačové sítě buďto na konec sítě nebo mezi dvě další zařízení např. switch a PC či IP telefon. Levý konektor RJ-45 je připojen do počítačové sítě a pravý ke koncovému zařízení.
- Stiskněte zelené tlačítko a držte, dokud se neobjeví úvodní obrazovka.

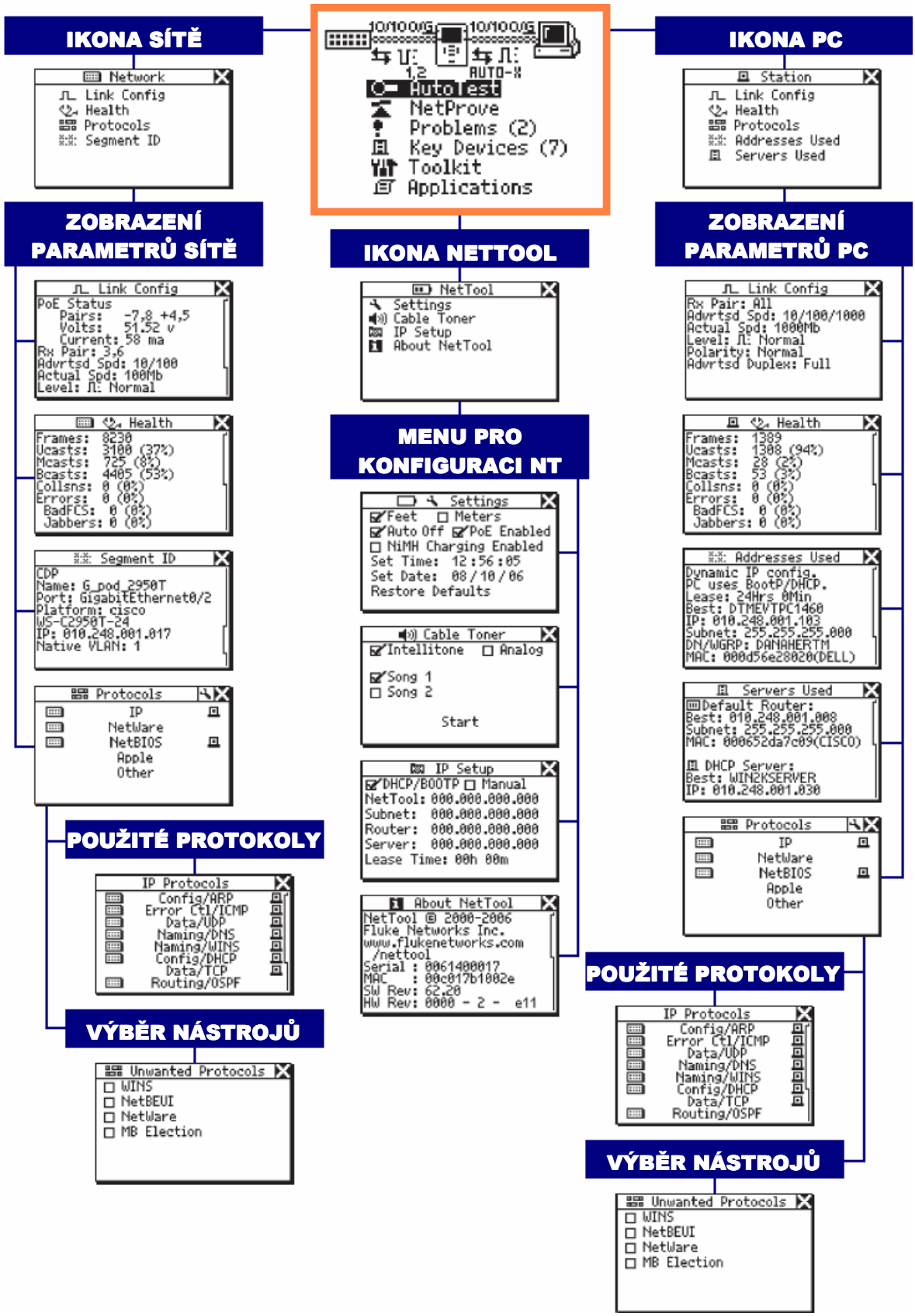
6.3 Ovládání:

- Tlačítkem **Select** potvrďte položku **AutoTest**, NetTool začne naslouchat síťovému provozu a během několika vteřin zobrazí diagnostiku sítě obr. 6.2.
- V NT se pohybujeme pomočí navigačních tlačítek (šipek), tlačítko **Select** slouží k výběru dané položky. Chceme-li se dostat o úroveň výše, najedeme na symbol křížku ☒ v pravém horním rohu a stiskneme **Select**.



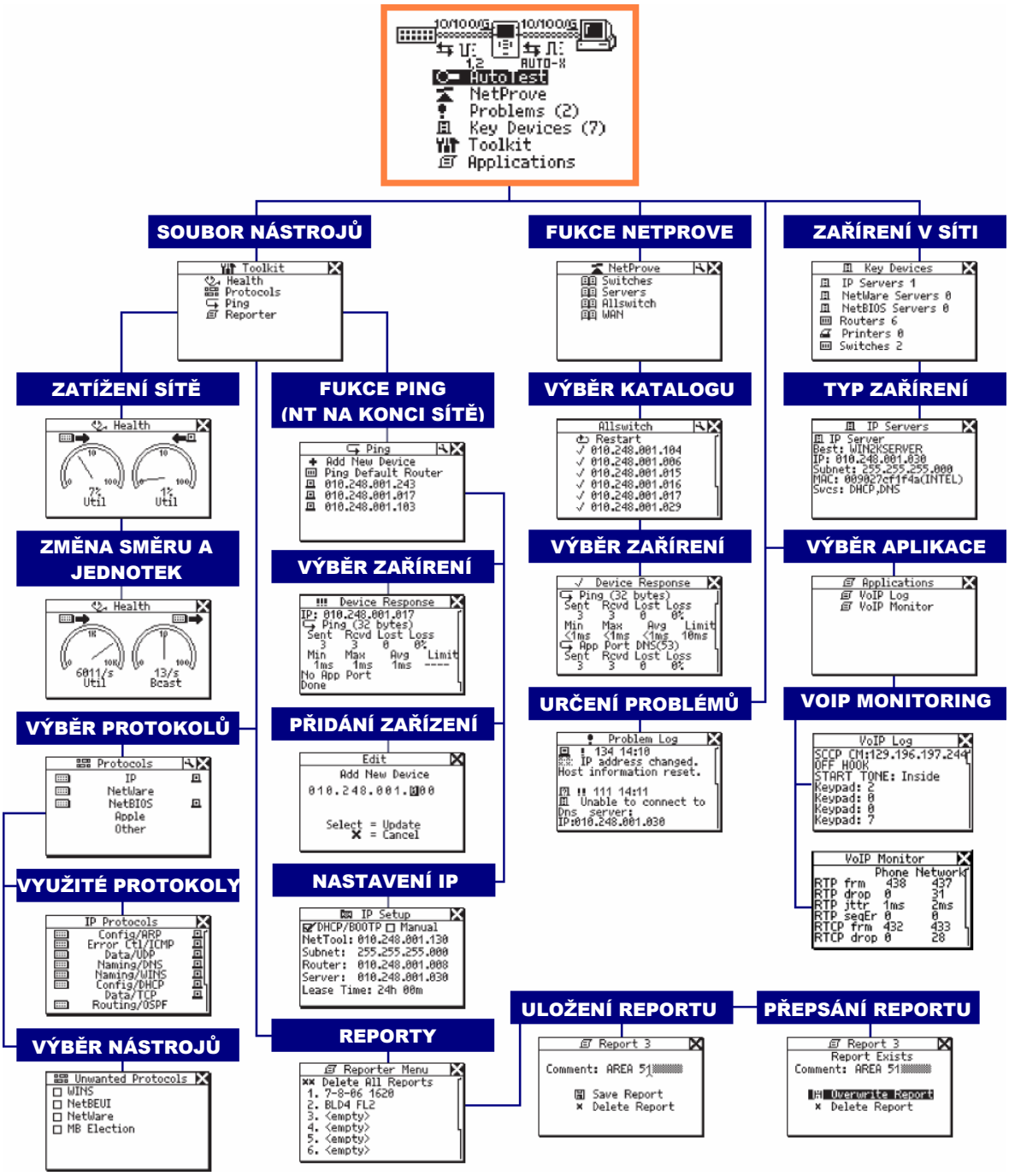
Obr. 6.2: Popis základních symbolů na displeji

6.3.1 Podrobný pohled na jednotlivé funkce pod ikonami sítě, NT a PC.



Obr. 6.3: Pohled na funkce NetTool analyzátoru pro zjištění informací o síti či PC

6.3.2 Podrobný pohled na jednotlivé funkce v hlavní nabídce NT



Obr. 6.4: Vyobrazení jednotlivých oken hlavní nabídky NetTool analyzátoru

6.4 Software pro připojení NetTool analyzátoru

NetTool Connect je jednoduchý program, který slouží k nastavení různých funkcí analyzátoru a exportu reportů. Jeno hlavní nabídka je na obr. 6.5, zahrnuje následující položky:

Obr. 6.5: Hlavní nabídka obslužného programu NT

Reports – Slouží k vytvoření zprávy o měření. Reporty jsou uloženy v NT a mohou být snadno exportovány. Buď uloženy v elektronické podobě ve formátu PDF, HTML a RAW, nebo přímo vytisknuty na papír.

NetProve – Slouží k ověření správné funkčnosti sítě. Můžeme zde nadefinovat až 10 různých testovacích katalogů. V katalogu se nastaví jednotlivá zařízení, jejichž správnou funkci chceme ověřit. Zařízení se definují DNS názvem nebo pevně stanovenou IP adresou.

Port Monitor – Zde se nastavují jednotlivé porty a k nim přiřazené protokoly, které chceme v síti analyzovat. Jednotlivé uvažované porty se vyberou z celkového seznamu a nahrají do NT analyzátoru.

802.1X – Nastavení autentizace NT pro síť využívající řízený přístup.

Update – Slouží k aktualizaci nahrání poslední verze softwaru či firmwaru přímo z internetových stránek výrobce.

Capture – Tato funkce zachytí aktuální obrazovku NT analyzátoru a uloží ji v podobě obrázku na pevný disk.

Personalize – Umožní uživateli nahrát do NT analyzátoru svou vlastní úvodní obrazovku, která se zobrazí při zapnutí přístroje.

Date/Time – Slouží k synchronizaci aktuálního data a času NT analyzátoru s počítačem.

Options – Umožňuje do NT nainstalovat další volitelné vlastnosti pomocí webu výrobce.

ZÁVĚR

V teoretické části této diplomové práce je podrobně popsána problematika zabývající se virtuálními sítěmi. Prezentuji zde síťový model TCP/IP využívaný v každé běžné počítačové síti a jeho vrstvové rozložení. Následuje popis komunikace v jednotlivých vrstvách a jim odpovídající přenosové protokoly. Čtenář je také obeznámen s IP telefonií, dnes velmi populární, a s komunikačními protokoly, které využívá.

V části praktické jsem navrhnul virtuální počítačovou síť, která je vhodná pro monitorování a analýzu běžného síťového provozu. Na přepínači jsou nastaveny dvě virtuální počítačové sítě, které slouží pro provoz osobních počítačů a IP telefonů v laboratoři. Následně jsem navrhnul a vypracoval laboratorní úlohu sloužící k výuce virtuálních sítí. Zadání úlohy je určeno přímo k měření a studenti by měli být schopni realizovat úlohu zcela samostatně s využitím této diplomové práce. Vzorový protokol poslouží vyučujícímu pro porovnání výsledků jednotlivých studentů.

Síťový provoz byl monitorován pomocí softwarového analyzátoru ClearSight a hardwarového Fluke NeTool Serie II, které umožňují zachycení provozu odesílaných a přijímaných e-mailů, uploadu a downloadu dat z FTP serveru a hovorů uskutečněných prostřednictvím IP telefonů.

Měření probíhala převážně v reálném čase, což umožňovalo sledovat okamžité změny využívání přenosových cest. Oba analyzátory mají velmi užitečnou funkci exportu naměřených a analyzovaných dat v podobě vlastnoručně nadefinovaných reportů. Tyto mohou být dále prezentovány v elektronické či papírové formě.

K analyzátorům jsou zpracovány přehledné manuály popisující jejich základní funkce a ovládání. Usnadní tak práci běžnému uživateli.

LITERATURA

[1] LAMPA, Petr, *Gigabitové páteřní sítě* [online], 1998, [cit. 2008-06-11]. Dostupný z WWW: < http://www.fit.vutbr.cz/~lampa/papers/giga98b.html.en >.

[2] *Wikipedia: The free enciclopedia: IEEE 802.1Q* [online], 2008. Dostupný z WWW: <http://en.wikipedia.org/wiki/IEEE_802.1Q>.

[3] CISCO, *Inter-Switch Link and IEEE 802.1Q Frame Format* [online], 2006. Dostupný z WWW: <http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094665.shtml>.

[4] IETF, RFC Pages, *A TCP/IP Tutorial,* [online], 1991. Dostupný z WWW: <http://www.ietf.org/rfc/rfc1180.txt>.

[5] *Wikipedie: Otevřená encyklopedie: Sada protokolů Internetu,* [online], 2008. Dostupný z WWW: <http://cs.wikipedia.org/wiki/TCP/IP>

[6] POLÍVKA, Michal. *Systém pro detekci útoku.* Brno, 2007, [cit. 2008-06-11]. Vedoucí diplomové práce Ing. Ivo Lattenberg Ph. D.

[7] PETERKA, Jiří. *Síťový model TCP/IP,* [online], 2006. Dostupný z WWW: <http://www.earchiv.cz/a92/a231c110.php3>.

[8] *Wikipedie: Otevřená encyklopedie: UDP,* [online], 2008, [cit. 2008-06-11]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/UDP>.

[9] IETF, RFC Pages, *The Lightweight User Datagram Protocol,* [online], 2004. Dostupný z WWW: <http://www.ietf.org/rfc/rfc3828.txt>.

[10] KAVICKÝ, David. *Optimalizace datových sítí pro přenos hlasu.* Brno, 2005. Vedoucí diplomové práce doc. Ing. Vladislav Škorpil, CSc.

[11] *Wikipedie: Otevřená encyklopedie: Voice over Internet Protocol,* [online], 2008, [cit. 2008-06-11]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Voip>.

[12] IETF, RFC Pages, *SIP: Session Initiation Protocol*, [online], 1999. Dostupný z WWW: <http://www.ietf.org/rfc/rfc2543.txt>

[13] PUŽMANOVÁ, Rita. *Moderní komunikační sítě A-Z.* Computer Press, Brno 2007

[14] IETF, RFC Pages, *RTP: A Transport Protocol for Real-Time Applications*, [online], 2003. Dostupný z WWW: <http://www.ietf.org/rfc/rfc3550.txt?number=3550>

[15] IETF, RFC Pages, *Real Time Control Protocol (RTCP)*, [online], 2003. Dostupný z WWW: <http://www.ietf.org/rfc/rfc3605.txt>

[16] *Telefonní systém 3CX pro Windows* [online]. 2008. Dostupný z WWW: <http://www.3cx.cz/>.

[17] *ClearSight Analyzer* [online]. 2008 [cit. 2008-06-11]. Dostupný z WWW: <http://www.clearsightnet.com/pages/products-analyzer.php>.

[18] *NetTool Series II* [online]. 2008 [cit. 2008-06-11]. Dostupný z WWW: <http://www.fluketestery.cz/produkty/nettool-serie-2.html>.

SEZNAM OBRÁZKŮ

SEZNAM POUŽITÝCH ZKRATEK

ACK - ACKnowledgment code

ATM - Asynchronous Transfer Mode

b - bit

B - Byte

CFI - Canonical Format Indicator

CRC - Cyclic Redundancy Check

DA - Destination Address

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

FTP - File Transfer Protocol

HTTP - Hyper Text Transfer Protocol

HW - Hardware

ICMP - Internet Control Message Protocol

IM - Instant Messaging

IP - Internet Protocol

IPsec - IP security

JPEG - Joint Photographic Experts Group

L/T - Length/Type

LAN - Local Area Network

MAC - Media Access Control

MGCP - Media Gateway Control Protocol

MPEG - Moving Picture Experts Group

NAT - Network Address Translation

NT - NetTool Serie II

OS - Operační Systém

PBX - Private Branch eXchange

PC - Personal Computer

PDF - Portable Document Format

PoE - Power over Ethernet

POP - Post Office protokol

PSTN - Public Switched Telephone Network

QoS - Quality of Service

RSVP - Ressource ReSerVation Protocol

RTCP - Real-time Transport Control Protocol

RTF - Rich Text Format

RTP - Real-time Transport Protocol

RTSP - Real Time Streaming Protokol

SA - Source Address

SDP - Session Description Protocol

SFD - Start of Frame Delimiter

SFD - Start of Frame Delimiter

SIP - Session Initiation Protocol

SMB - Server Message Block

SMTP - Simple Mail Transfer Protokol

SQL - Structured Query Language

SRTP - Secure Real-time Transport Protocol

SW - Software

TCI - Tag Control Information

TCP - Transmission Control Protocol

TPID - Tag Protocol IDentifier

UDP - User Datagram protokol

URL - Unifor Ressource Locator

VID - VLAN ID

VLAN - Virtuální LAN

VoIP - Voice over Internet Protocol

VPN - Virtual Private Network

WAN - Wide Area Network

PŘÍLOHA 1

Report zobrazující komunikaci a využití protokolů během VoIP hovoru

NetTool Reports

Live Data Report

Report Date: 5/22/08 15:58:04

Host

Link Configuration
Rx Pair: 1,2
Advertised Speed: N/A
Actual Speed: 100Mb
Link Level: 0 Low
Polarity: Normal
Advertised Duplex: Full/Half
Actual Duplex: Full
Measured Duplex: N/A
Power Over Ethernet: None

Addresses Used
IP: 147.229.148.137
IP Subnet: 255.255.254.000
MAC: 0013f7687bff(SMC)

Dynamic IP Configuration. PC uses BootPC/DHCP.
Lease: 24Hrs 0Min

Servers Used
Dhcp Server
IP: 147.229.148.020
IP Subnet: 255.255.254.000

Dns Server
IP: 147.229.072.010

Default Router
IP: 147.229.148.001
IP Subnet: 255.255.254.000

Health
Total Frames: 4633
Broadcasts: 3 (1%)
Multicasts: 0 (0%)
Unicasts: 4630 (99%)
Collisions: 0 (0%)
Errors: 0 (0%)
FCS: 0 (0%)
Undersize: 0 (0%)
Jabbers: 0 (0%)
Ghosts: 0 (0%)
Oversize: 0 (0%)
RxSymbol: 0 (0%)
Alignment: 0 (0%)
Length error: 0 (0%)

Network

Link Configuration
Rx Pair: 3,6
Advertised Speed: N/A
Actual Speed: 100Mb
Link Level: 4 Normal
Polarity: Normal
Advertised Duplex: Full/Half
Actual Duplex: Full
Measured Duplex: N/A
Power Over Ethernet: None

Segment ID
IP Networks
147.229.xxx.xxx
147.229.148.xxx
147.229.128.xxx

IPX Encapsulations
802.2

CDP
Platform: HP 2626
Name: HP ProCurve Switch 2626(001185-a3bb00)
Port: 3
IP: 127.000.000.001

Health
Total Frames: 5040
Broadcasts: 239 (4%)
Multicasts: 163 (3%)
Unicasts: 4638 (92%)
Collisions: 0 (0%)
Errors: 0 (0%)

FCS: 0 (0%)
Undersize: 0 (0%)
Jabbers: 0 (0%)
Ghosts: 0 (0%)
Oversize: 0 (0%)
RxSymbol: 0 (0%)
Alignment: 0 (0%)
Length error: 0 (0%)

Protocols

IP Protocols

Protocol	Network (Left Side RJ)	Host (Right Side RJ)
Config/ARP	x	x
Error Ctl/ICMP	x	x
Data/UDP	x	x
Data/TCP	x	
Naming/WINS	x	x
Config/DHCP	x	x

IPX Protocols

Protocol	Network (Left Side RJ)	Host (Right Side RJ)
Config/SAP	x	

NetBIOS Protocols

Protocol	Network (Left Side RJ)	Host (Right Side RJ)
Session	x	
Name Server	x	
NetBIOS over IP	x	

Apple Protocols

Protocol	Network (Left Side RJ)	Host (Right Side RJ)
Data/DDP	x	
Config/ZIP	x	

Other Protocols

none detected

Key Devices

IP Servers

2 IP Servers seen

IP Services Seen: DHCP, DNS, IP WINS

IP: 147.229.148.020
IP Subnet: 255.255.254.000
Services: DHCP

IP: 147.229.072.010
Services: DNS, IP WINS

Routers

1 Routers seen

Routers Seen: Static

IP: 147.229.148.001
IP Subnet: 255.255.254.000
Services: Static

VoIP Monitor

	Phone	Network
RTP Frames	807	842
RTP Dropped Frames	1074	1092
RTP Jitter	2ms	2ms
RTP Sequence Errors	84	54
RTCP Frame	0	0
RTCP Dropped Frames	0	0
RTCP Jitter	0s	0s

VoIP Log

05/22/08 15:50:06
INVITE sip:1001@term.ut
ko.feec.vutbr.cz SIP/2.
SIP/2.0 100 Trying
SIP/2.0 180 Ringing
SIP/2.0 200 OK
SIP gw:147.229.148.022
SIP RTP port:60000
ACK sip:1002@147.229.14
8.22:5060 SIP/2.0
Call Setup:210ms
RTP streaming...
147.229.148.137:60000

VLAN:untag TOS:0xa0
147.229.148.135:60000
VLAN:untag TOS:0xa0
BYE sip:1002@147.229.14
8.22:5060 SIP/2.0
>RTP cnt:807fr
Jitter:2ms
Arrival Avg:9ms
Min:8ms Max:11ms
Drop:1074fr
DropBurst:479ms
<RTP cnt:842fr
Jitter:2ms
Arrival Avg:9ms
Min:7ms Max:10ms
Drop:1092fr
DropBurst:800ms
Call Complete

PŘÍLOHA 2

Report zobrazující komunikaci a využití protokolů při běžném provozu

NetTool Reports

Live Data Report

Report Date: 5/22/08 16:10:52

Host

Link Configuration
Rx Pair: 3,6
Advertised Speed: N/A
Actual Speed: 100Mb
Link Level: 5 Normal
Polarity: Normal
Advertised Duplex: Full/Half
Actual Duplex: Full
Measured Duplex: Full
Power Over Ethernet: None

Addresses Used
IP: 147.229.148.127
IP Subnet: 255.255.254.000
NetBIOS Host: DA352530
NetBIOS Group: SKUPINA
MAC: 001a4d5b854f

Dynamic IP Configuration. PC uses BootPC/DHCP.
Lease: 24Hrs 0Min

Servers Used
Dhcp Server
IP: 147.229.148.020
IP Subnet: 255.255.254.000

Dns Server
IP: 147.229.072.010
DNS: kos.feec.vutbr.cz

Wins Server
IP: 147.229.072.010

DNS: kos.feec.vutbr.cz

Http Server
IP: 147.229.072.010
DNS: kos.feec.vutbr.cz

Default Router
IP: 147.229.148.001
IP Subnet: 255.255.254.000

Health
Total Frames: 10719
Broadcasts: 22 (1%)
Multicasts: 4 (1%)
Unicasts: 10693 (99%)
Collisions: 0 (0%)
Errors: 0 (0%)
FCS: 0 (0%)
Undersize: 0 (0%)
Jabbers: 0 (0%)
Ghosts: 0 (0%)
Oversize: 0 (0%)
RxSymbol: 0 (0%)
Alignment: 0 (0%)
Length error: 0 (0%)

Network

Link Configuration
Rx Pair: 3,6
Advertised Speed: N/A
Actual Speed: 100Mb
Link Level: 3 Normal
Polarity: Normal
Advertised Duplex: Full/Half
Actual Duplex: Full
Measured Duplex: Full
Power Over Ethernet: None

Segment ID
IP Networks
147.229.xxx.xxx
147.229.144.xxx
147.229.148.xxx

IPX Encapsulations
802.2

Health
Total Frames: 23021
Broadcasts: 229 (1%)

Multicasts: 145 (1%)
Unicasts: 22647 (98%)
Collisions: 0 (0%)
Errors: 0 (0%)
FCS: 0 (0%)
Undersize: 0 (0%)
Jabbers: 0 (0%)
Ghosts: 0 (0%)
Oversize: 0 (0%)
RxSymbol: 0 (0%)
Alignment: 0 (0%)
Length error: 0 (0%)

Protocols

IP Protocols

Protocol	Network (Left Side RJ)	Host (Right Side RJ)
Config/ARP	x	x
Data/UDP	x	x
Data/TCP	x	x
Ping/ECHO	x	x
Naming/DNS	x	x
Naming/WINS	x	x
Config/DHCP	x	x

IPX Protocols

Protocol	Network (Left Side RJ)	Host (Right Side RJ)
Config/SAP	x	

NetBIOS Protocols

Protocol	Network (Left Side RJ)	Host (Right Side RJ)
Session	x	x
Name Server	x	x
NetBIOS over IP	x	x

Apple Protocols

Protocol	Network (Left Side RJ)	Host (Right Side RJ)
Data/DDP	x	
Config/ZIP	x	

Other Protocols
none detected

Key Devices

IP Servers
4 IP Servers seen
IP Services Seen: DHCP, DNS, IP WINS, HTTP

IP: 147.229.148.020
IP Subnet: 255.255.254.000
Services: DHCP

IP: 147.229.072.010
DNS: kos.feec.vutbr.cz
Services: DNS, IP WINS, HTTP

IP: 147.229.144.010
Services: DHCP

IP: 147.229.003.010
Services: DNS

Routers
1 Routers seen
Routers Seen: Static

IP: 147.229.148.001
IP Subnet: 255.255.254.000
Services: Static